WIRELESS G 4-PORT VPN ROUTER USER MANUAL

Model 524582

INTELLINET NETWORK SOLUTIONS

BRINGING NETWORKS TO LIFE

INT-524582-UM-0309-01

INTRODUCTION

The INTELLINET NETWORK SOLUTIONS Wireless G 4-Port VPN Router lets you experience fast speeds as you surf the Web, download music or photos, and play online games. This wireless router works with 802.11g as well as the older 802.11b products, and also includes a four-port 10/100 LAN switch so you can connect using network cable or go wireless to satisfy all your needs.

The router provides IPSec VPN gateway functionality that allows remote users to access your office network securely. It also helps you to build secure network tunnels between your branch office and headquarters.

And because keeping intruders out of your network can be a challenge, this feature-rich wireless router is designed to make that challenge easier. It includes a true SPI (Stateful Packet Inspection) firewall that secures your network against hackers. With Network Address Translation (NAT) to shield your networked devices from intruders, Denial of Service (DoS) attack prevention to avert potential threats by scanning incoming traffic, and WEP, WPA and WPA2 encryption to conceal your information on the wireless LAN from eavesdroppers, you can rest assured that you have taken the necessary precautions to protect the data on your network.

Follow the instructions in this manual and you'll soon be enjoying the benefits of these additional features:

- Compatible with all common DSL and cable Internet service providers
- Up to 54 Mbps network data transfer rate
- Supports Wireless Access Point, Repeater and Bridging modes
- VPN server support (PPTP, IPSec and L2TP protocols)
- QoS (Quality of Service) bandwidth management
- DHCP server assigns IP addresses for all LAN users
- Supports DDNS (dynamic DNS)
- Supports UPnP (Universal Plug and Play)
- Supports virtual server, port forwarding and DMZ (demilitarized zone)
- VPN pass-through for IPSec and PPTP
- IPSec VPN gateway (ESP, IKE)
- Provides 3DES and AES encryption algorithms
- Provides MD5 and SHA1 authentication algorithms
- Content control through URL filter
- Supports MAC filtering for wireless clients
- Remote management function
- Easy installation through Web-based user interface
- Configuration backup and restore via Web-based user interface
- Firmware updates via Web-based user interface
- Lifetime Warranty

Regulatory Statements

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment to an outlet on a different circuit.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This equipment must be installed and operated in accordance with the provided instructions, and a minimum of 20 cm spacing must be provided between a computer-mounted antenna and a person's body (excluding extremities of hands, wrists and feet) during wireless modes of operation.

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of Directive 1999/5/EC of the European Parliament and the Council of March 9, 1999, on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces Directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety
This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All FCC and computer manufacturer guidelines must therefore be followed at all times to ensure the safe use of the equipment.

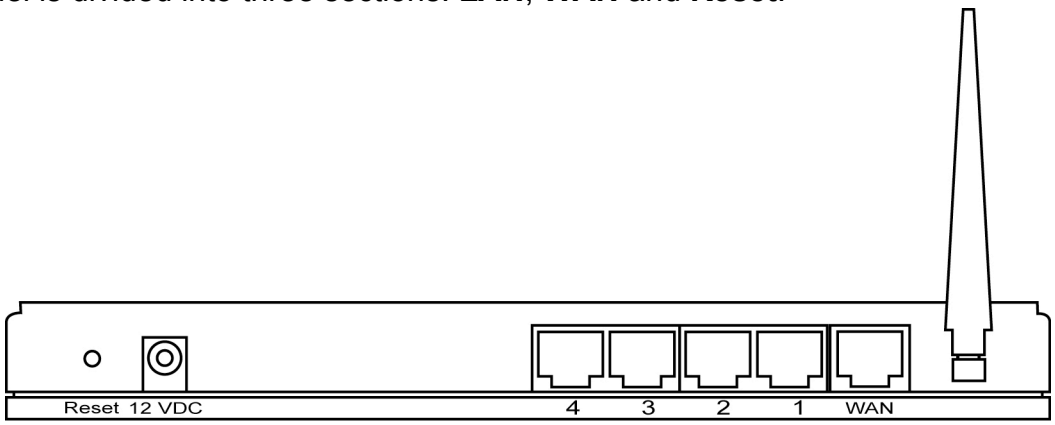
EU Countries Intended for Use
The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the U.K. The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland. (EU countries *not* intended for use: none.)

IMPORTANT NOTICE: It has recently been discovered that the WAN Idle Time Out auto-disconnect function may not work due to abnormal activities of some network application software, computer viruses or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. This function also may not work with some Internet service providers. If you decide to enable this function, make sure it works properly the first time, especially if your ISP charges are based on connection time. Due to the many uncontrollable issues, we do not guarantee the WAN Idle Time Out auto-disconnect function will always work: To avoid resulting fees charged by your ISP, don't enable this function.

1 HARDWARE

1.1 Back Panel

The diagram below shows the broadband router's back panel. The router's back panel is divided into three sections: **LAN**, **WAN** and **Reset**:



Local Area Network (LAN)
The router's four LAN ports (1-4) are where you connect your LAN's PCs, printer servers, hubs and switches, etc.

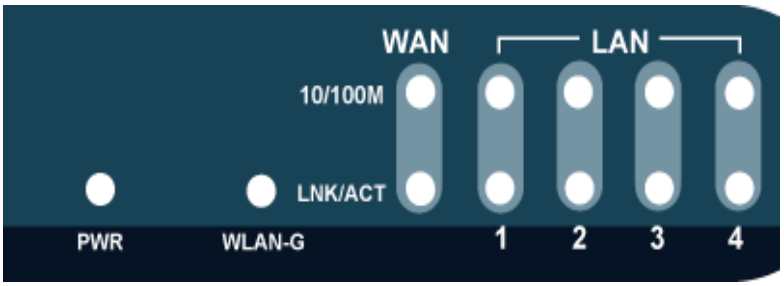
Wide Area Network (WAN)
The WAN port connects to your xDSL or cable modem and is linked to the Internet.

Reset
The Reset button allows you to do one of two things:

- If problems occur with your router, press the Reset button with a pencil tip (for less than 4 seconds) and the router will re-boot itself, keeping your original configurations.
- If problems persist or you experience extreme problems or you forgot your password, press the Reset button for more than 4 seconds and the router will reset itself to the factory defaults. ***NOTE:*** Your original configurations will be replaced with the factory default settings.

1.2 Front Panel

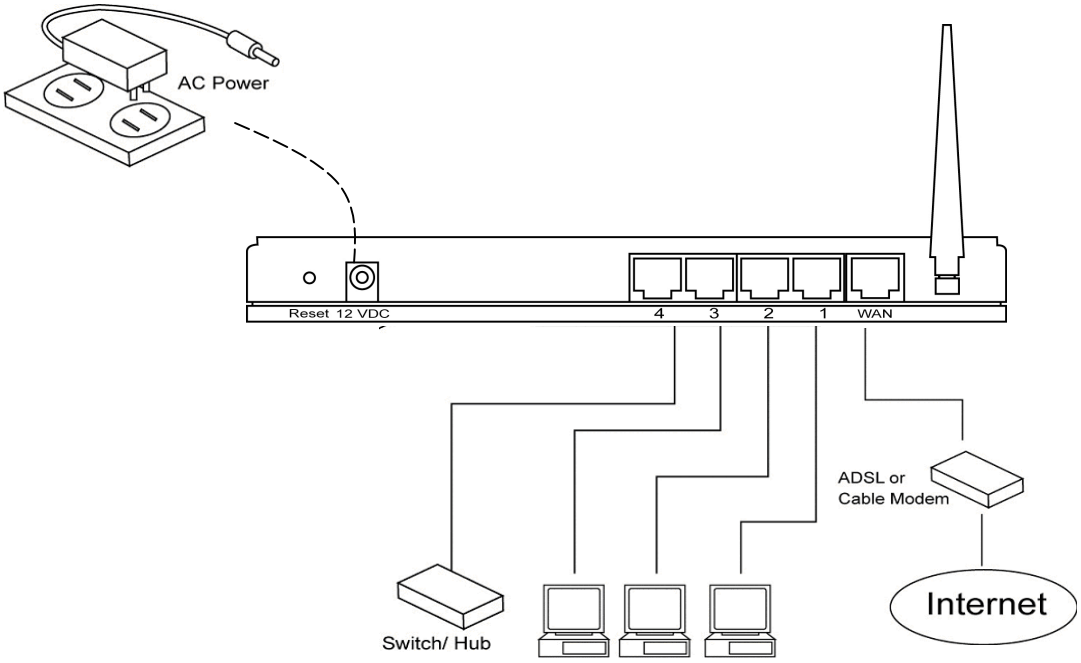
LED lights inform you of the router's current status.



LED	Status	Description
PWR	On	Router's power supply is on.
WLAN-G	On	Wireless LAN has been activated.
	Off	Wireless LAN is disabled.
	Flashing	Wireless LAN has activity (ACT): data being sent.
WAN10/100M	On	WAN port 100 Mbps is connected.
	Off	WAN port 10 Mbps is connected.
WAN LNK/ACT	On	WAN is connected.
	Off	No WAN connection.
	Flashing	WAN port has activity (ACT): data being sent.
LAN 10/100M (1-4)	On	LAN port 100 Mbps is connected.
	Off	LAN port 10 Mbps is connected.
LAN LNK/ACT (1-4)	On	LAN is connected.
	Off	No LAN connection.
	Flashing	LAN port has activity (ACT): data being sent.

1.3 Setup Diagram

The image below depicts a typical setup for a local area network (LAN).



2 QUICK SETUP

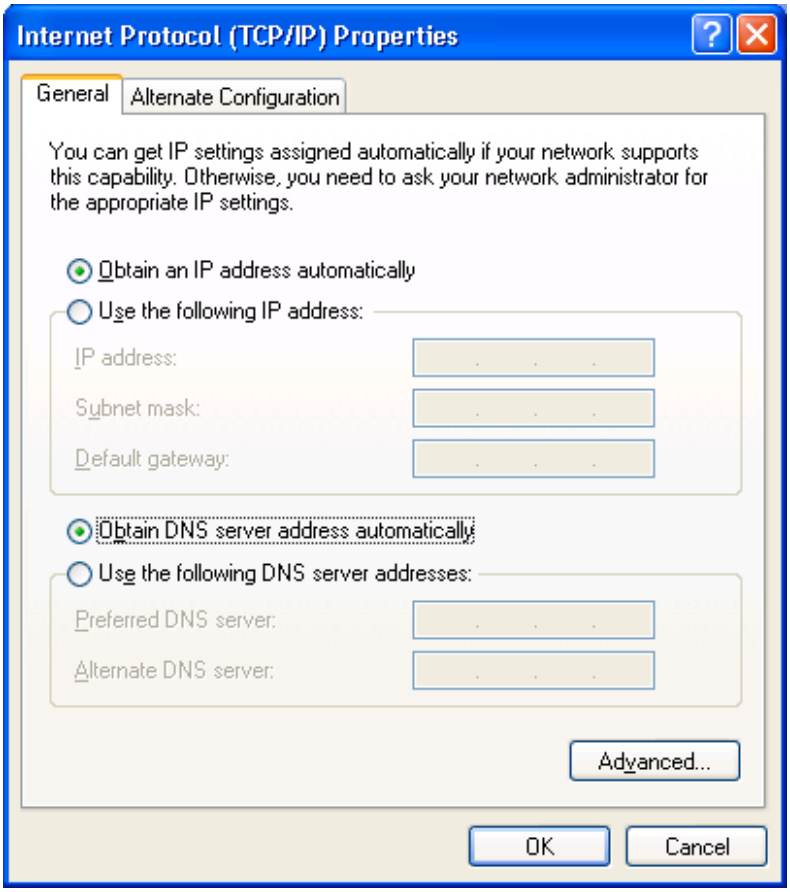
2.1 Getting Started

Once you have your network configured (see the sample setup diagram in Section 1.3 above), you need to set your LAN PC clients so they can obtain an IP address automatically. All LAN clients require an IP address: Just like a street address, it allows LAN clients to find one another. (If you have already configured your PC to obtain an IP automatically, proceed to Login below.)

By default, the router's DHCP is on, which means that you can obtain an IP address automatically once you've configured your PC to do so. The procedures for Windows XP and Vista operating systems are presented below: For other operating systems (Macintosh, Sun, etc.), follow the manufacturer's instructions.

Windows XP

1. Click the Start button and select Settings, then click Network Connections.
2 Double-click the Local Area Connection icon to display its window.
3. Check your list of Network Components. You should see "Internet Protocol [TCP/IP]" on your list. Select it and click "Properties."

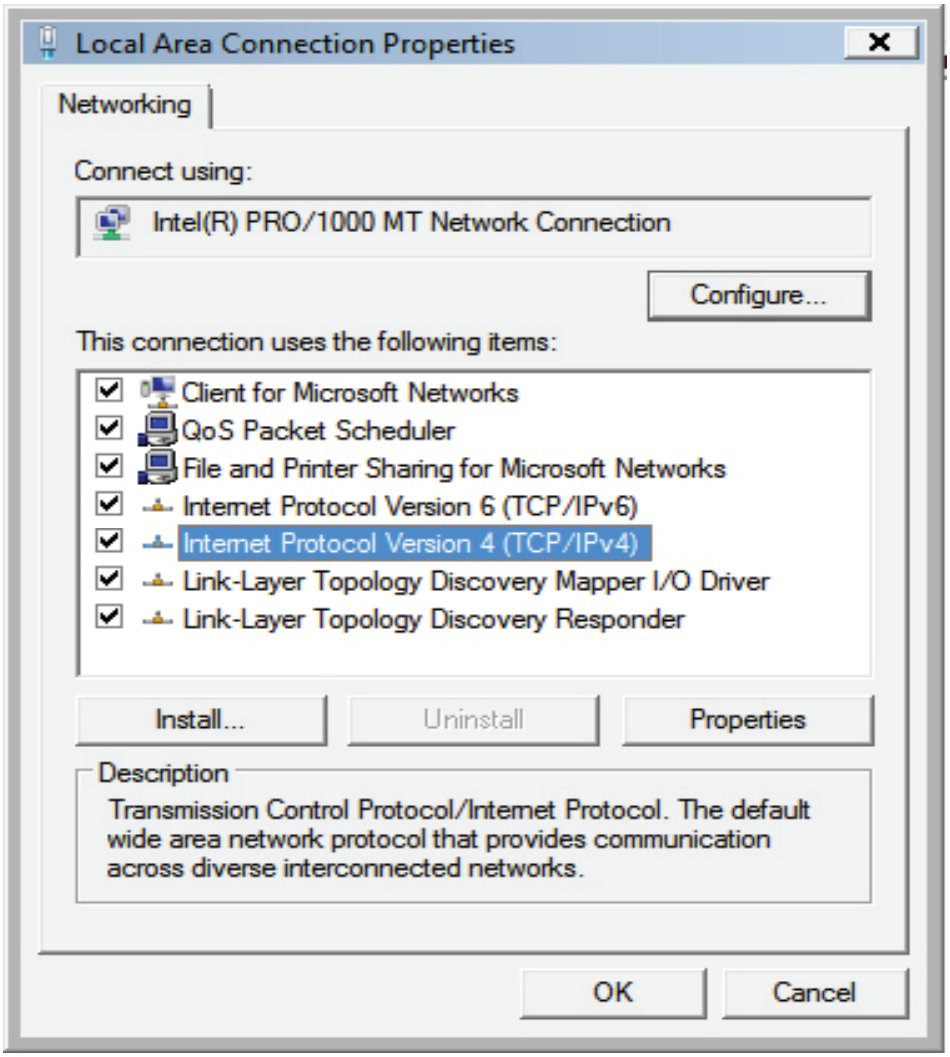


4. In the Internet Protocol (TCP/IP) Properties window, select “Obtain an IP address automatically” and “Obtain DNS server address automatically.”
5. Click “OK” to confirm the setting. Your PC will now obtain an IP address automatically. Proceed to the Login section below.

NOTE: Make sure that the Wireless G VPN Router’s DHCP server is the only DHCP server available on your LAN.

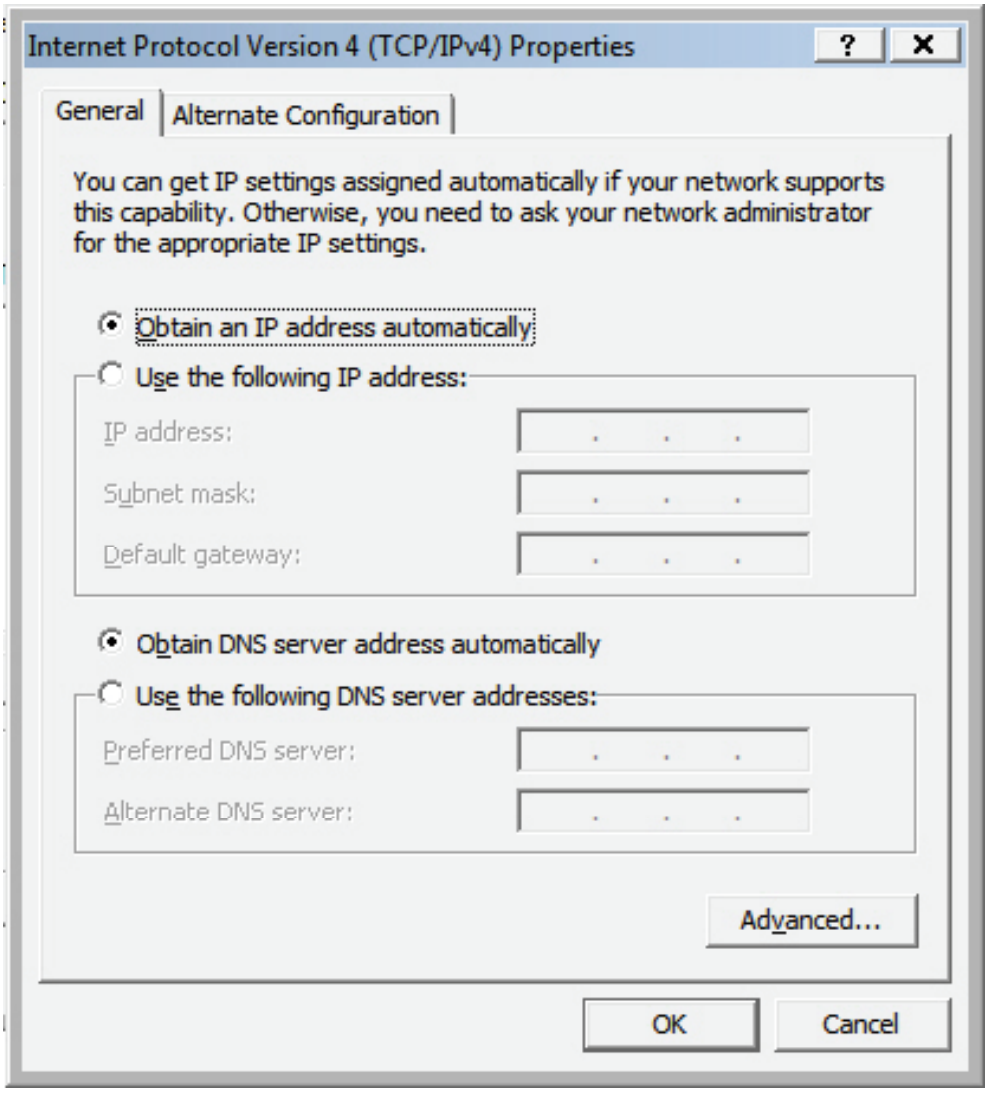
Windows Vista

1. Click “Start,” then click “Control Panel.”
2. Click “View Network Status and Tasks,” then click “Manage Network Connections.”
3. Right-click “Local Area Network,” then select “Properties.”
4. With the Local Area Connection Properties screen displayed, select “Internet Protocol Version 4 (TCP/IPv4) and click “Properties.”



5. In the Internet Protocol (TCP/IPv4) Properties window, select “Obtain an IP address automatically” and “Obtain DNS server address automatically.”
6. Click “OK” to confirm the setting. Your PC will now obtain an IP address automatically. Proceed to the Login section below.

NOTE: Make sure that the Wireless G VPN Router’s DHCP server is the only DHCP server available on your LAN.



Login

Once you have configured your PCs to obtain an IP address automatically, the Wireless G VPN Router's DHCP server will automatically give your LAN clients an IP address. By default, the DHCP server is enabled to do this. To see if you have obtained an IP address, see the Appendix near the back of this manual.

NOTE: As stated in the procedures above, make sure that the Wireless G VPN Router's DHCP server is the only DHCP server available on your LAN. If there is another DHCP on your network, you'll need to switch one of the DHCP servers off. (To disable the Wireless G VPN Router's DHCP server, see Section 3.3.)

With your IP address(es) obtained from your router, follow these three steps:

1. Enter the default IP address 192.168.2.1 (the router's IP address) into your PC's Web browser and press <Enter>.

2. When the login screen displays, fill in the "User Name" and "Password" fields, then click "OK" to log in.

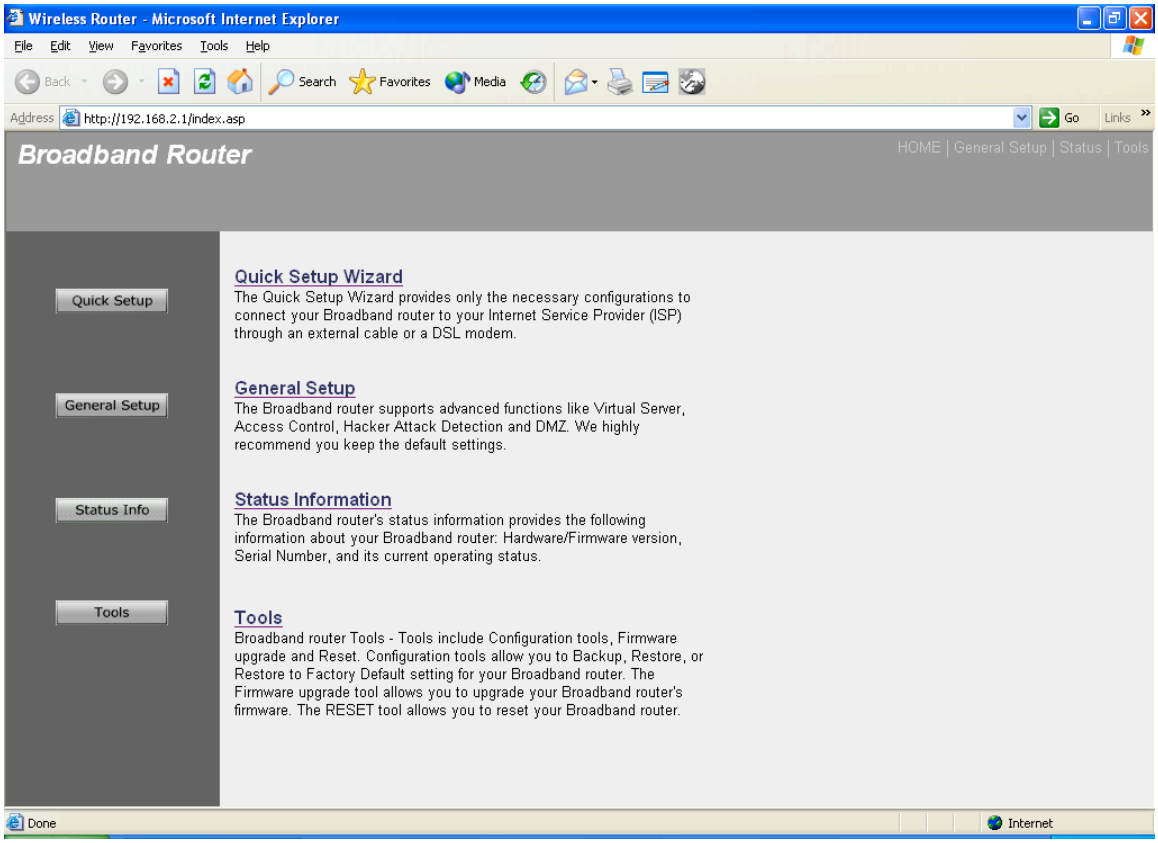
NOTE: By default, the username is "admin" and the password is "1234." For security reasons, it's recommended that you change the password as soon as possible (see Section 3.1.2).

3. When the HOME page screen displays (below), click "Quick Setup" on the left-hand menu bar to go directly to the Quick Setup Wizard, which will show you how to start using the Wireless G VPN Router as on Internet access device only. Otherwise, you can click one of the other three primary menu options — General Setup, Status Information and Tools — and proceed with more detailed settings and network configurations.

General Setup (Section 3)
If you want to use more advanced features that this router has to offer, then you'll need to configure the Quick Setup Wizard and the General Setup section. Alternatively, you can just configure the General Setup section, since the General Setup/WAN and the Quick Setup Wizard contain the same configurations.

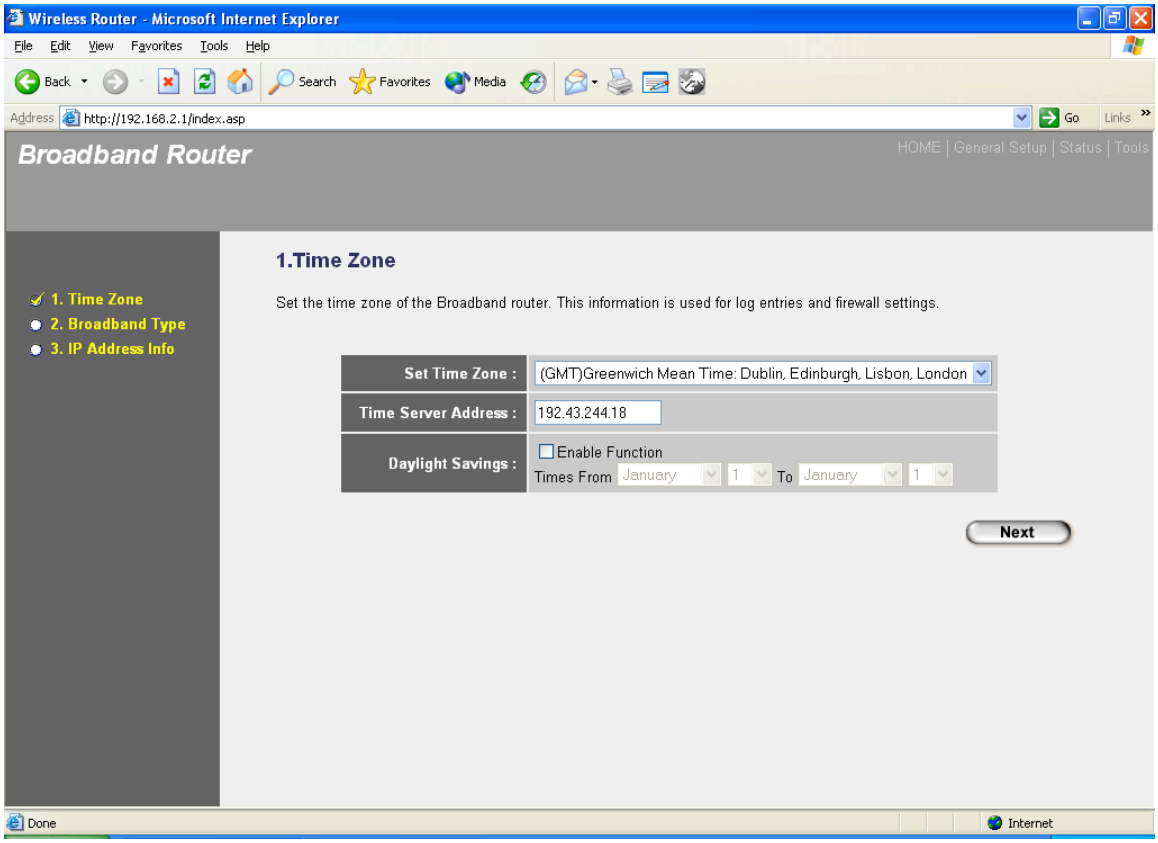
Status Information (Section 4)
This is for monitoring the router's current status information only.

Tools (Section 5)
If you want to reset the router (because of problems) or save your configurations or upgrade the firmware, this is the place to do this.



2.2 Quick Setup Wizard

If you only want to start using the broadband router as an Internet access device, then you only need to configure the screens in this Quick Setup Wizard section.



2.2.1 Time Zone

The Time Zone allows your router to base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

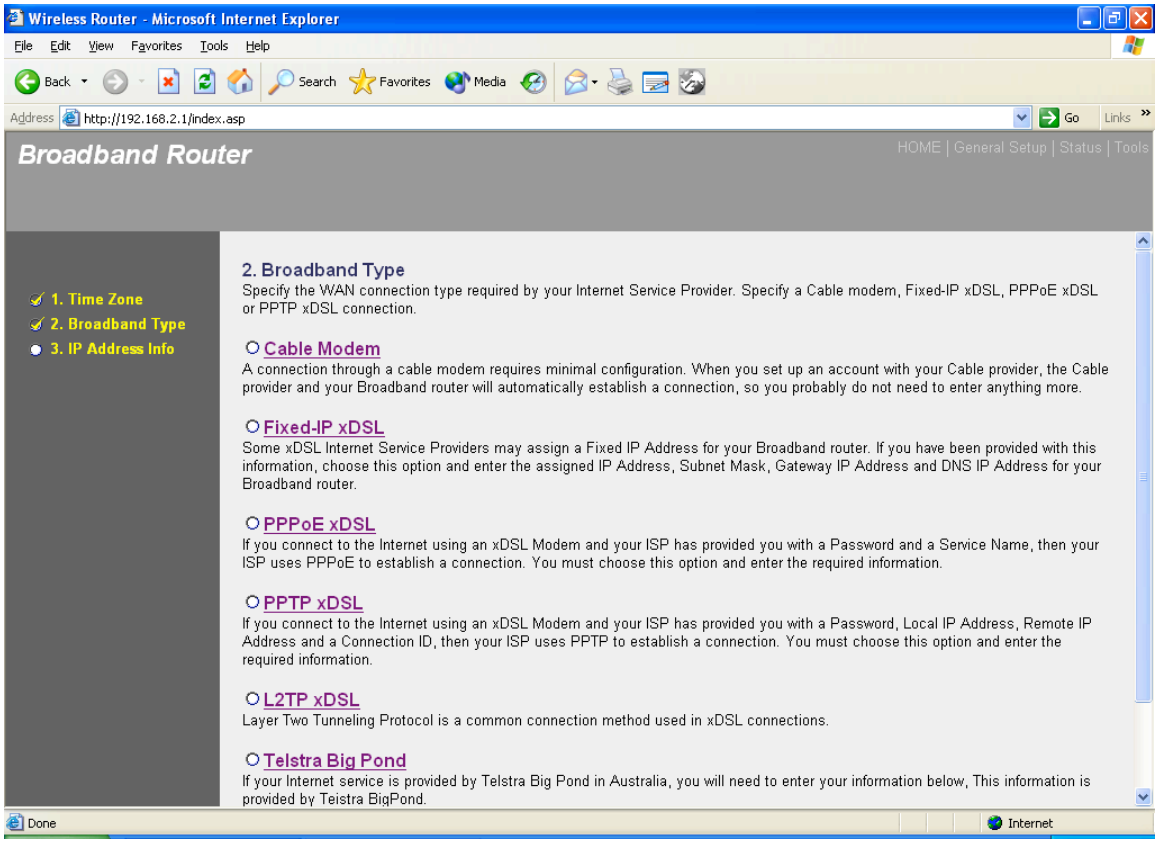
Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	You can manually assign time server address if the default time server dose not work.
Enable Daylight Saving	The router can also take Daylight Saving into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).

Start Daylight Saving Time	Select the period in which you wish to start daylight Saving Time.
End Daylight Saving Time	Select the period in which you wish to end Daylight Saving Time.

Click “Next.”

2.2.2 Broadband Type

In this section, you have to select one of four types of connections that you will be using to connect your router’s WAN port to your ISP (see screen below).
Note: Different ISPs require different methods of connecting to the Internet. Check with your ISP as to the type of connection it requires.



Menu	Description
2.2.2.1 Cable Modem	Your ISP will automatically give you an IP address
2.2.2.2 Fixed-IP xDSL	Your ISP has given you an IP address already
2.2.2.3 PPPoE	Your ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection.

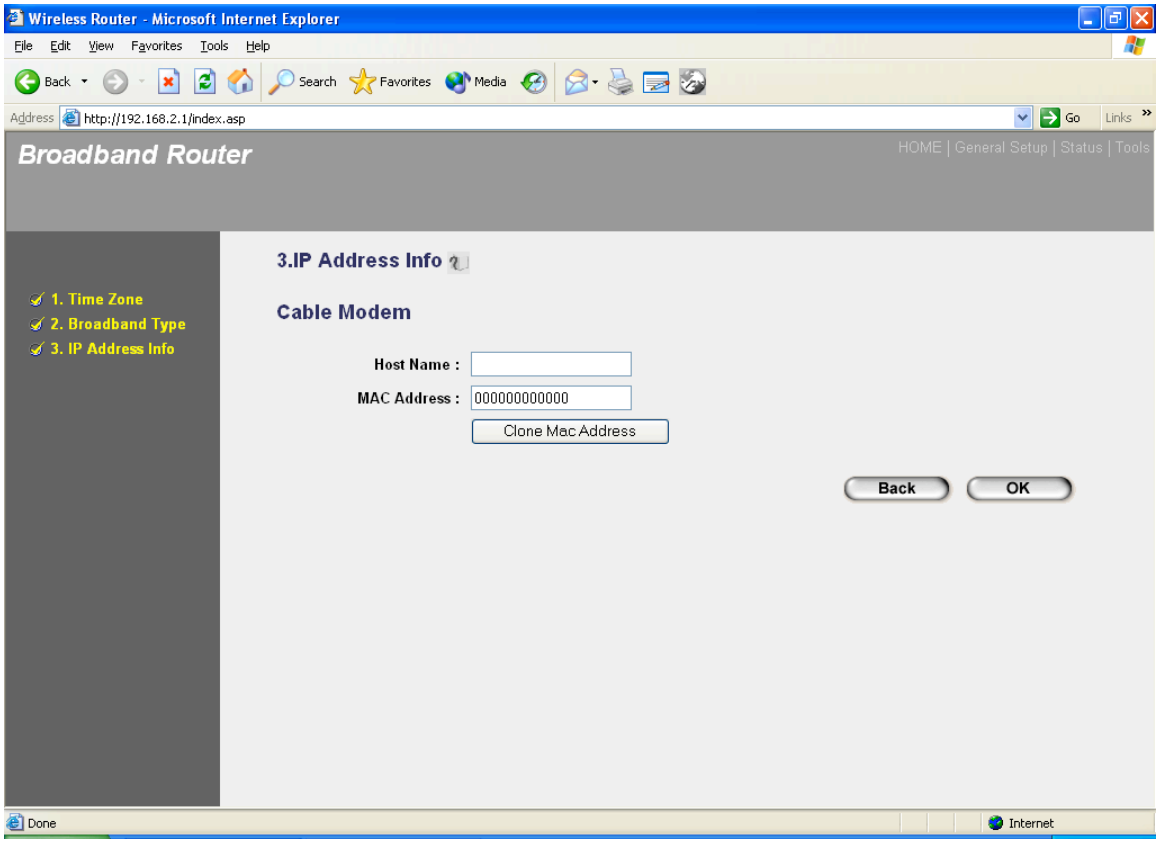
2.2.2.4 PPTP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
2.2.2.5 L2TP	Your ISP requires you to use a Layer Two Tunneling Protocol (L2TP) connection.
2.2.2.6 Telstra BigPond	This protocol is only used for Australia's ISP connection.

Click "Back" to return to the previous screen.

2.2.2.1 Cable Modem

Choose Cable Modem if your ISP will automatically give you an IP address. Some ISPs may also require that you fill in additional information, such as Host Name and MAC address (see screen below).

Note: The Host Name and MAC address section is *optional*. You can skip this section if your ISP does not require these settings for you to connect to the Internet.



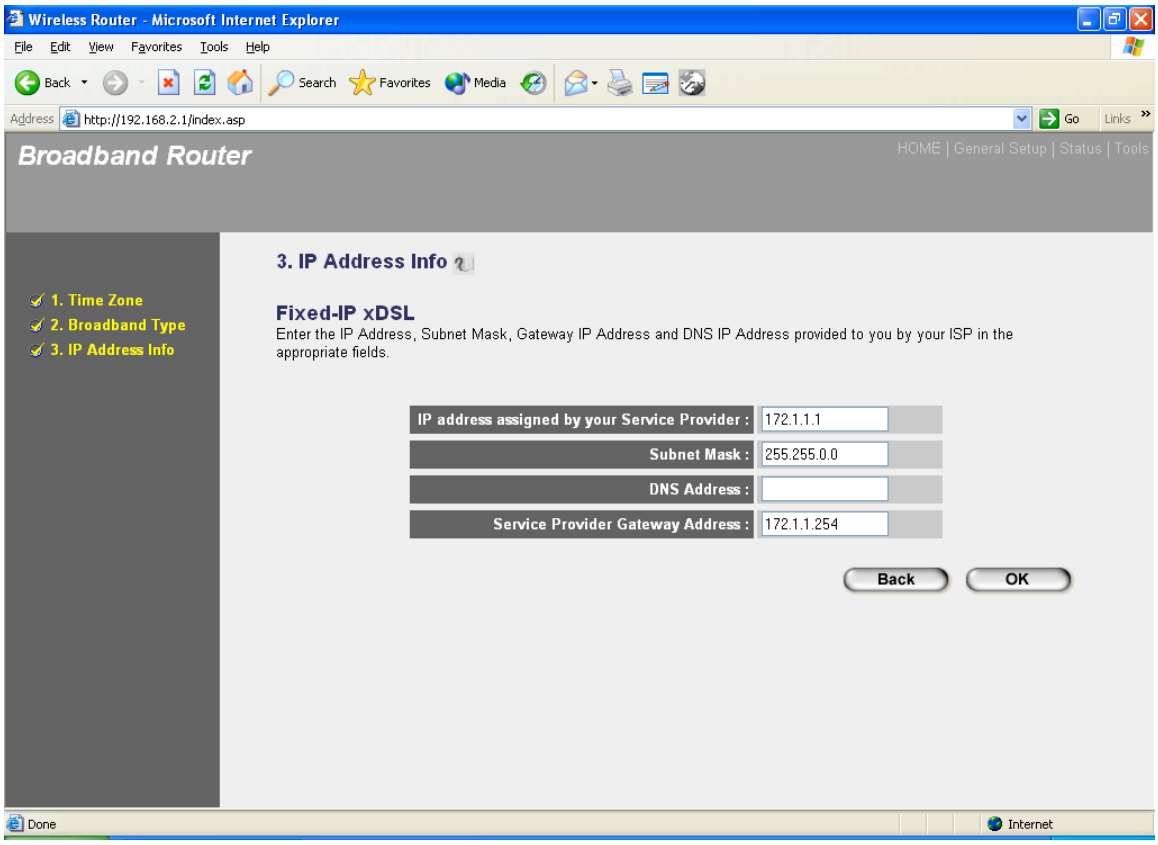
Parameters	Description

Host Name	If your ISP requires a Host Name, type in the host name provided by your ISP; otherwise, leave it blank if your ISP does not require a Host Name.
MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the "**Clone MAC Address"** button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC's MAC address, see Appendix A. (See Glossary for an explanation of MAC address.)

Click "OK**"** when you have finished the configuration above. You have completed the configuration for the Cable Modem connection. You can start using the router now.

2.2.2.2 Fixed-IP xDSL

Select Fixed-IP xDSL if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section.

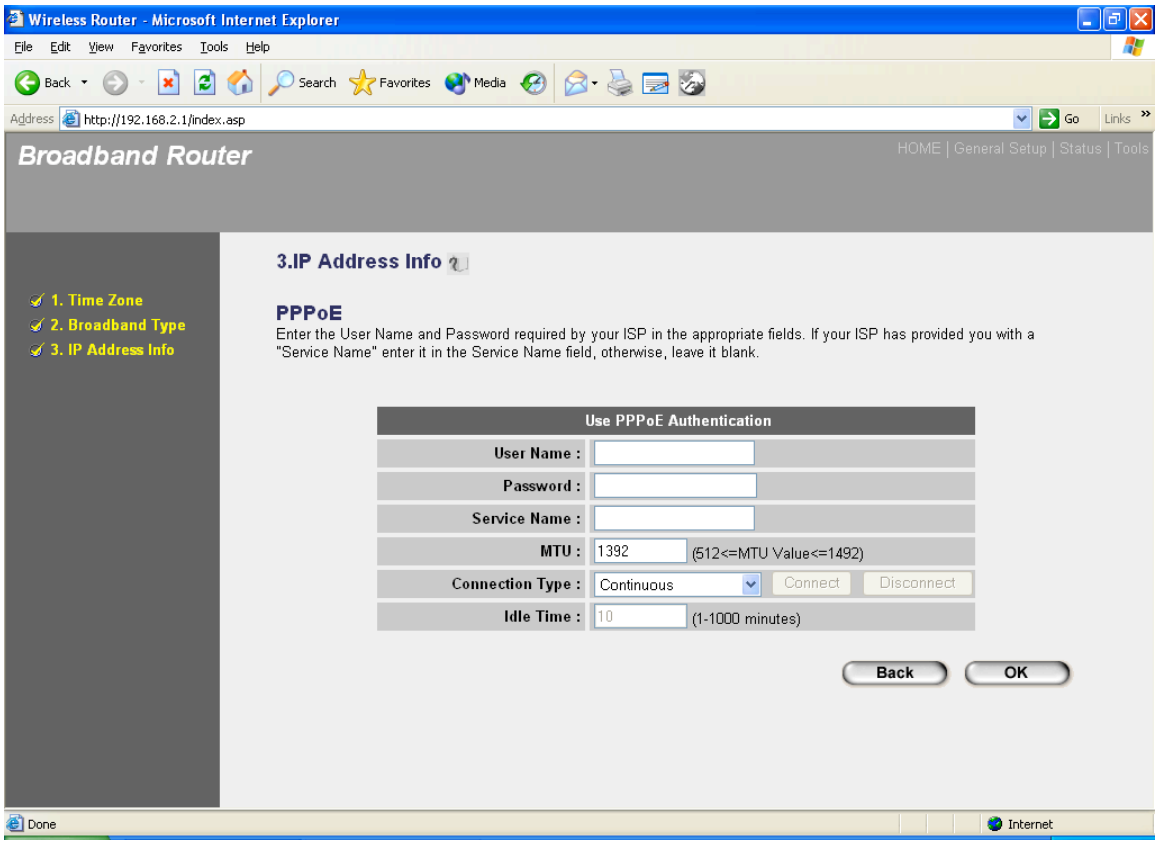


Parameters	Description
IP	This is the IP address that your ISP has given you.
Gateway IP	This is the ISP's IP address gateway.
DNS	This is the ISP's DNS server IP address.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g., 255.255.255.0).

Click "OK" when you have finished the configuration above. You have completed the configuration for the Fixed-IP x DSL connection. You can start using the router now.

2.2.2.3 PPPoE

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



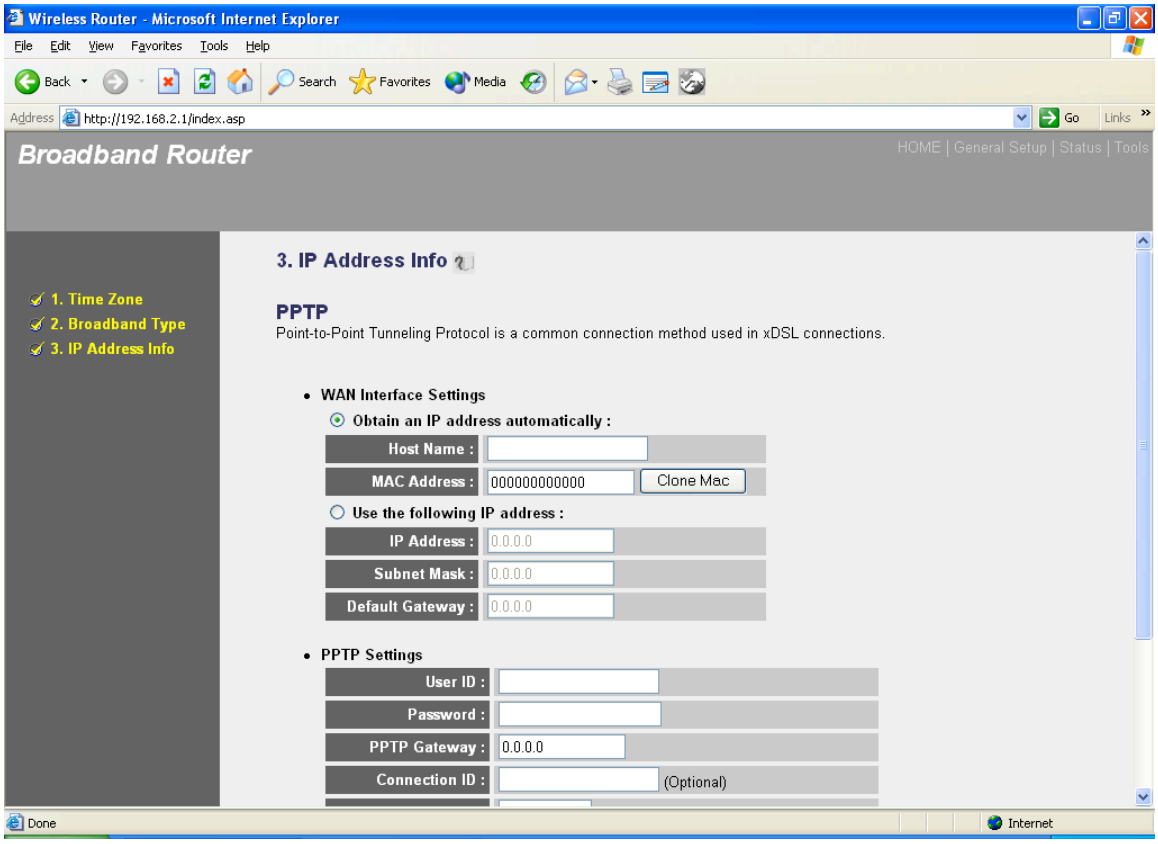
Parameter	Description
User Name	Enter the User Name provided by your ISP for the PPPoE connection.

Password	Enter the password provided by your ISP for the PPPoE connection
Service Name	This is optional. Enter the service name if your ISP requires it; otherwise, leave it blank.
MTU	Enter the MTU value provided by your ISP.
Connection Type	If you select “Continuous,” the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select “Connect On Demand,” the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the Idle Time. If you select “Manual,” the router will connect to the ISP only when you click “Connect” manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one is using the Internet) during this specified period, the router will automatically disconnect the connection with your ISP. **Note:** This “idle timeout” function may not work due to abnormal activities of some network application software, computer viruses or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. Turn off your computer when you are not using it. This function also may not work with some ISPs. Make sure this function can work properly when you use this function the first time, especially if your ISP charges you by time used.

Click “OK” when you have finished the configuration above. You have completed the configuration for the PPPoE connection. You can start using the router now.

2.2.2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



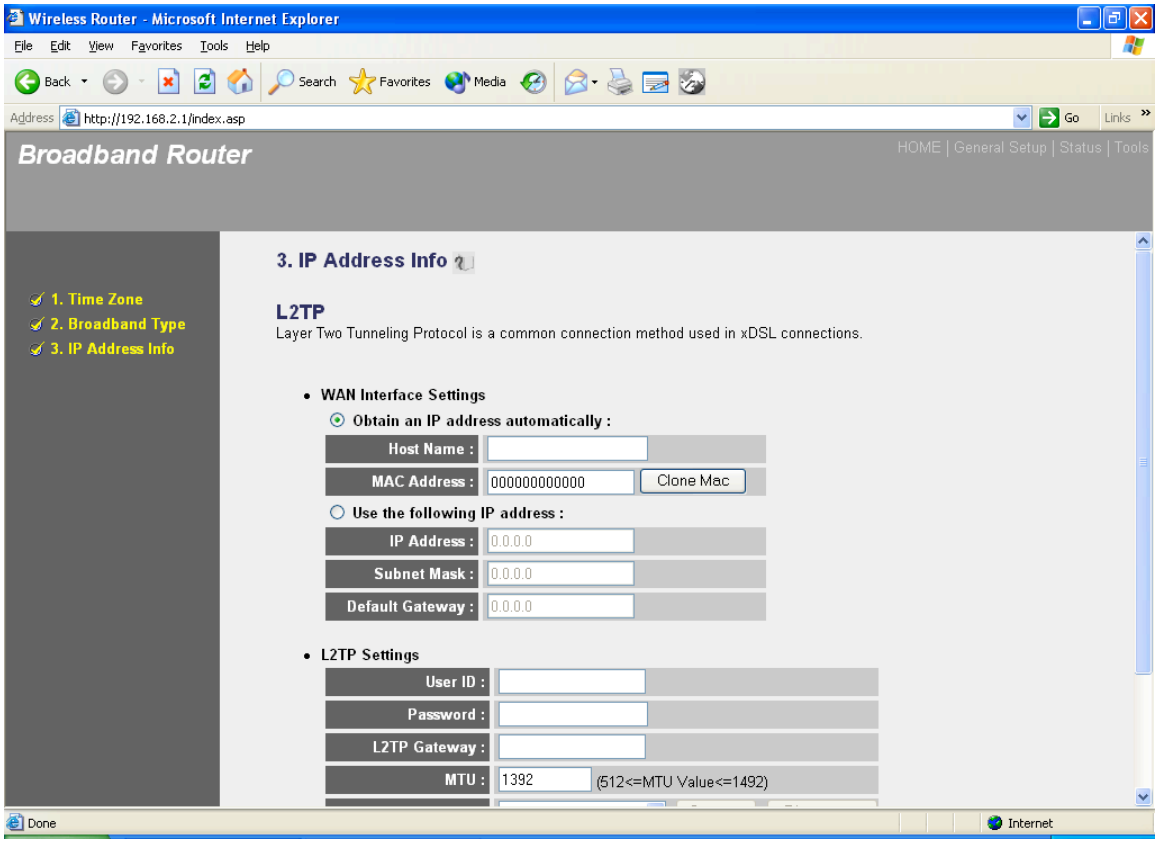
Parameter	Description
Obtain an IP address automatically	The ISP requires you to obtain an IP address by DHCP before connecting to the PPTP server.
Use the following IP address	The ISP give you a static IP to be used to connect to the PPTP server.
IP Address	This is the IP address that your ISP has given you to establish a PPTP connection.
Subnet Mask	Enter the subnet mask provided by your ISP (e.g., 255.255.255.0).
Gateway	Enter the IP address of the ISP gateway.
User ID	Enter the username provided by your ISP for the PPTP connection.
Password	Enter the password provided by your ISP for the PPTP connection.

PPTP Gateway	If your LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If you do not have a PPTP gateway, then enter the ISP's gateway IP address above.
Connection ID	This is the ID given by ISP. This is optional.
BEZEQ-ISRAEL	Select this item if you are using the service provided by Bezeq in Israel.
Connection Type	If you select "Continuous," the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select "Connect On Demand," the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the Idle Time. If you select "Manual," the router will connect to the ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one is using the Internet) throughout this specified period, then the router will automatically disconnect the connection with your ISP. **Note:** This "idle timeout" function may not work due to abnormal activities of some network application software, computer viruses or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. Turn off your computer when you are not using it. This function also may not work with some ISPs. Make sure this function can work properly when you use this function the first time, especially if your ISP charges you by time used.

Click "OK" when you have finished the configuration above. You have completed the configuration for the PPTP connection. You can start using the router now.

2.2.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



Parameter	Description
Obtain an IP address automatically	The ISP requires you to obtain an IP address by DHCP before connecting to the L2TP server.
MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the “Clone MAC Address” button to work). To find out the PC's MAC address, see Appendix A. (See Glossary for an explanation of MAC address.)
Use the following IP address	The ISP gives you a static IP to be used to connect to the L2TP server.

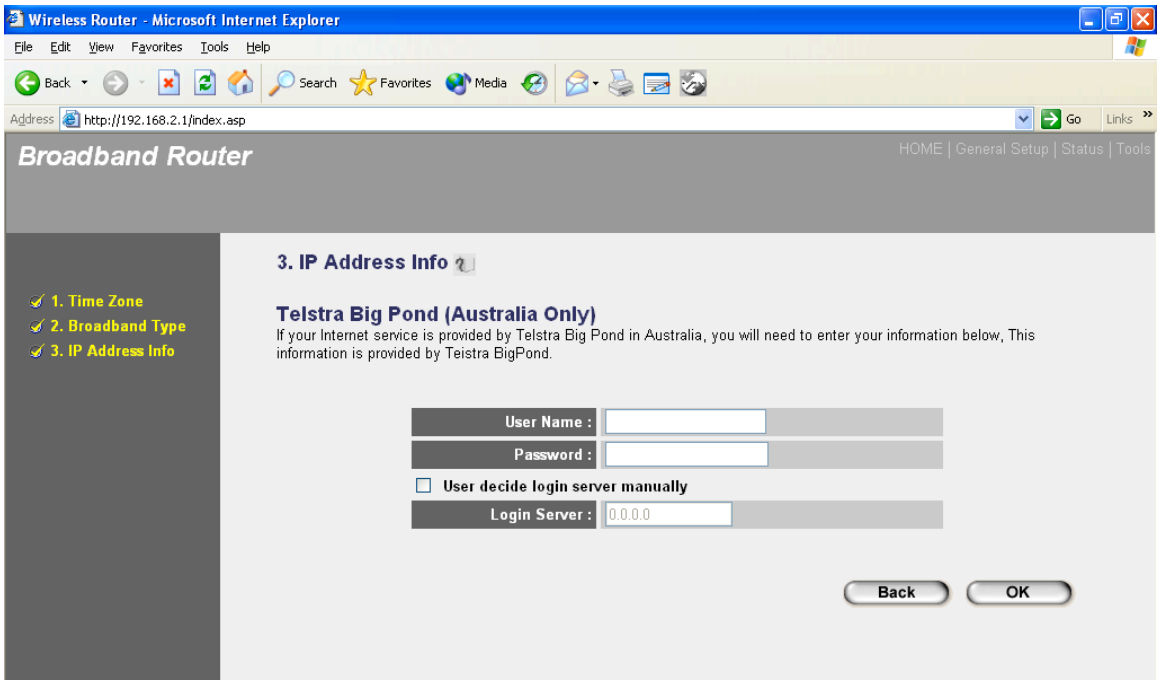
IP Address	This is the IP address that your ISP has given you to establish an L2TP connection.
Subnet Mask	Enter the subnet mask provided by your ISP (e.g., 255.255.255.0).
Gateway	Enter the IP address of the ISP gateway.
User ID	Enter the username provided by your ISP for the PPTP connection.
Password	Enter the Password provided by your ISP for the PPTP connection
L2TP Gateway	If your LAN has an L2TP gateway, then enter that L2TP gateway IP address here. If you do not have an L2TP gateway, enter the ISP's gateway IP address above.
MTU	Enter the MTU value provided by your ISP.
Connection Type	If you select "Continuous," the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select "Connect On Demand," the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the Idle Time. If you select "Manual," the router will connect to the ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one is using the Internet) throughout this specified period, then the router will automatically disconnect the connection with your ISP. **Note:** This "idle timeout" function may not work due to abnormal activities of some network application software, computer viruses or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. Turn off your computer when you are not using it. This function also may not

work with some ISPs. Make sure this function can work properly when you use this function the first time, especially if your ISP charges you by time used.

Click “OK” when you have finished the configuration above. You have completed the configuration for the L2TP connection. You can start using the router now.

2.2.2.6 Telstra BigPond

Select Telstra BigPond if your ISP requires the Telstra BigPond protocol to connect you to the Internet. Your ISP should provide all the information required in this section. Telstra BigPond protocol is used by the ISP in Australia.



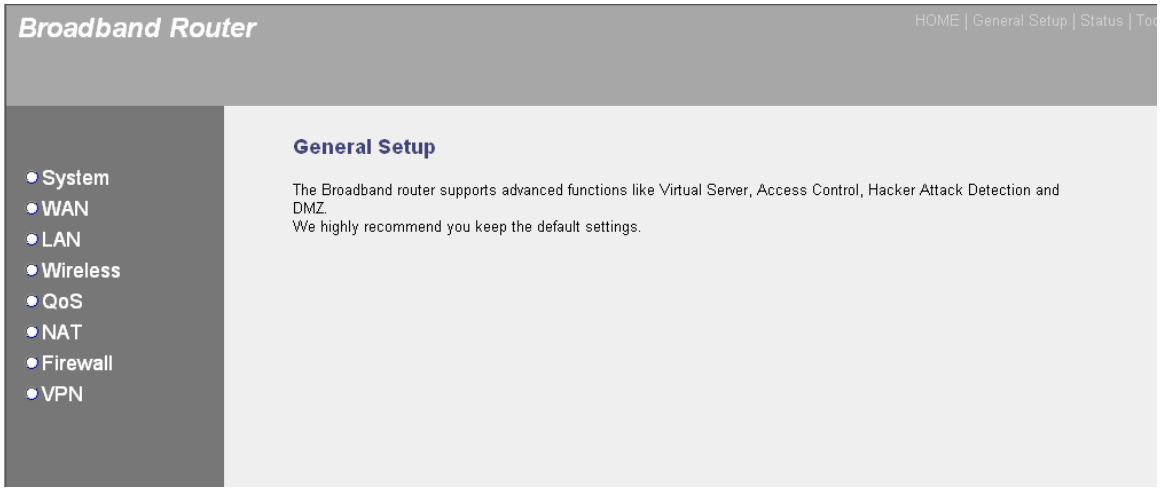
Parameter	Description
User Name	Enter the username provided by your ISP for the Telstra BigPond connection.
Password	Enter the password provided by your ISP for the Telstra BigPond connection.
User decide login server manually	Select if you want to assign the IP of Telstra BigPond’s login server manually.
Login Server	The IP of the login server.

Click “OK” when you have finished the configuration above. You have completed the configuration for the Telstra BigPond connection. You can start using the router now.

3 GENERAL SETUP

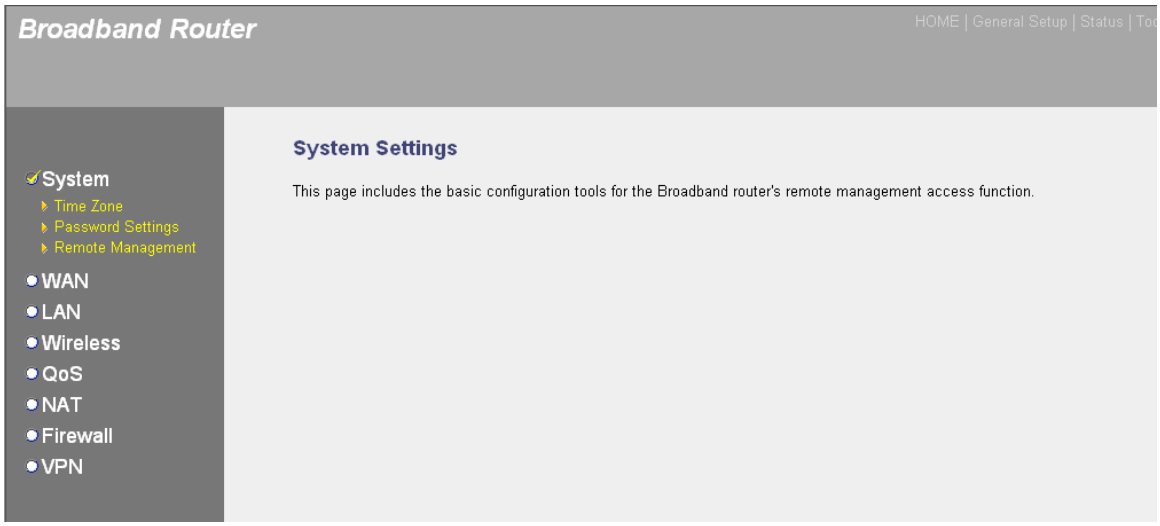
Once you click “General Setup” at the Home Page, you should see the screen below. If you have already configured the Quick Setup Wizard you do not need to configure anything thing in the General Setup screen to start using the Internet.

General Setup contains advanced features that allow you to configure the router to meet your network’s needs, such as: Wireless, Address Mapping, Virtual Server, Access Control, Hacker Attack Prevention, Special Applications and DMZ.



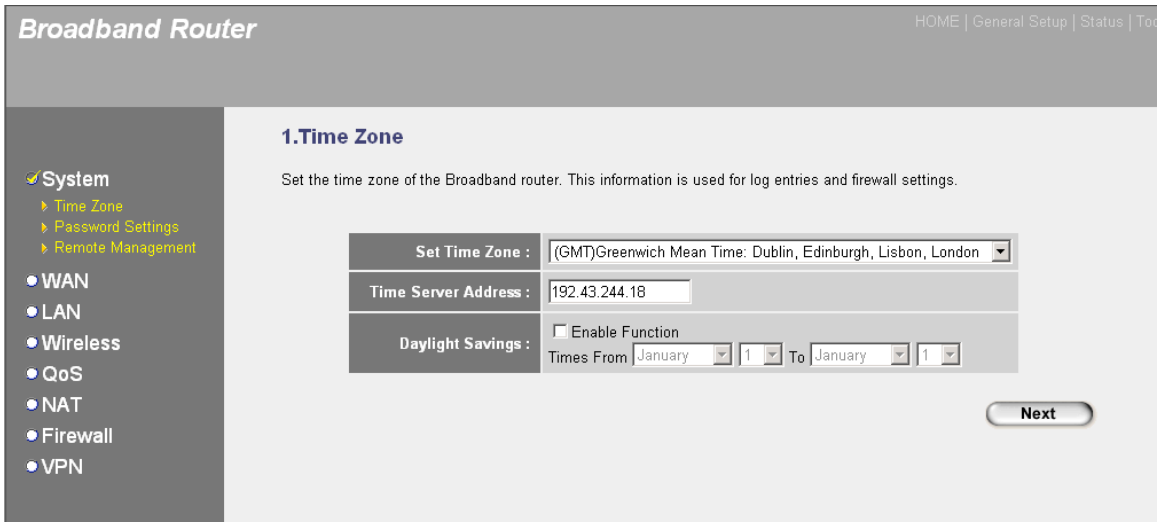
3.1 System

The system screen allows you to specify a time zone, to change the system password and to specify a remote management user for the broadband router.



3.1.1 Time Zone

Time Zone allows your router to reference or base its time on the settings configured here, which will affect functions such as log entries and firewall settings.

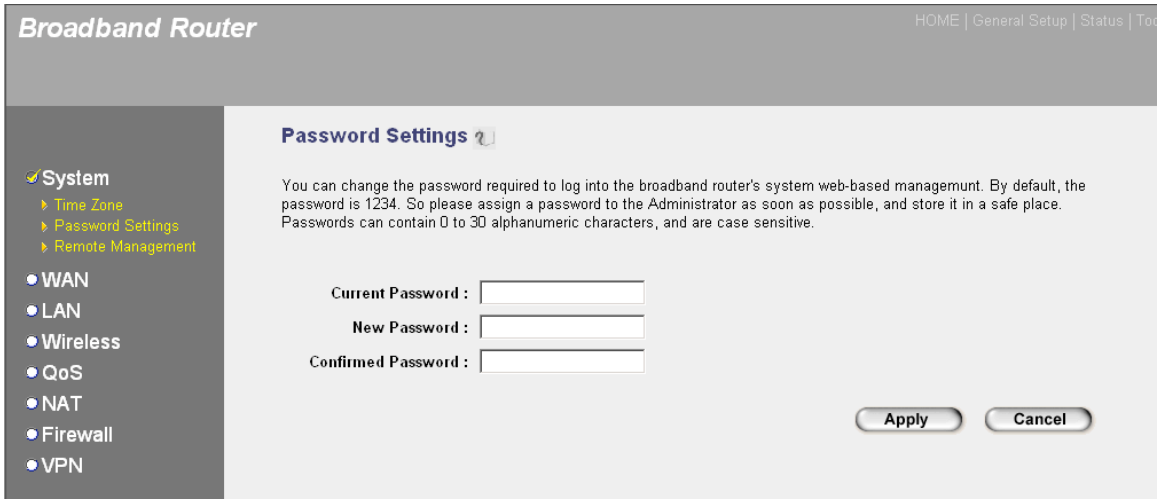


Parameter	Description
Set Time Zone	Select the time zone of the country you're in. The router will set its time based on your selection.
Time Server Address	The router default is "192.43.244.18."
Enable Daylight Saving	The router can also take Daylight Saving into account. To use this function, check the enable box to enable your Daylight Saving configuration (below).
Start Daylight Saving Time	Select the period in which you wish to start Daylight Saving Time.
End Daylight Saving Time	Select the period in which you wish to end Daylight Saving Time.

Click "Apply" at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

3.1.2 Password Settings

You can change the password required to log in to the broadband router's system Web-based management. By default, there is no password: Assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain up to 12 alphanumeric characters and are case sensitive.

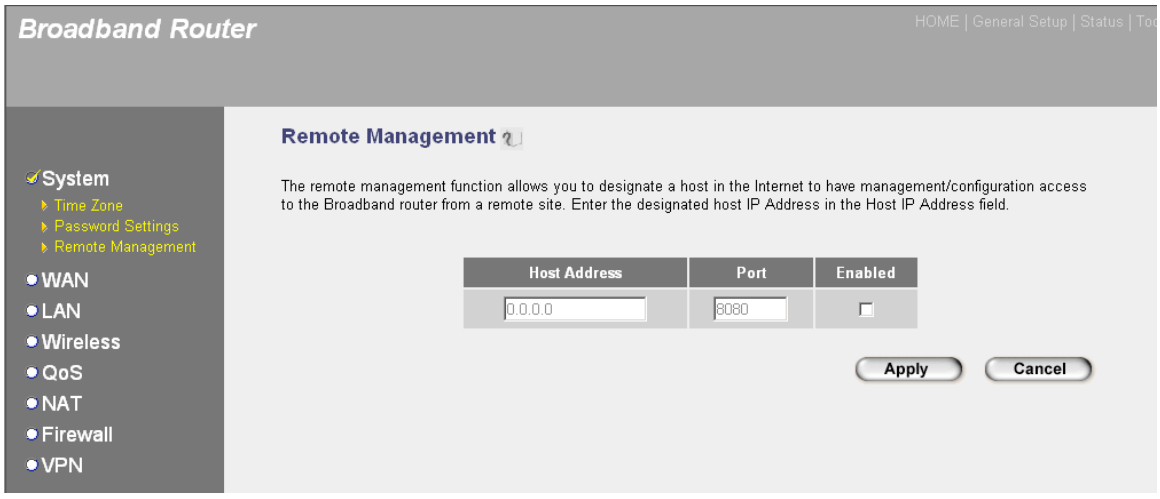


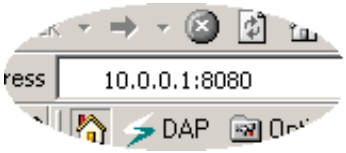
Parameter	Description
Current Password	Enter your current password for the remote management administrator to log in to your router. ***Note:*** By default there is no password.
New Password	Enter your new password.
Confirmed Password	Enter your new password again for verification. ***Note:*** If you forget your password, you'll have to reset the router to the factory defaults (no password) with the Reset button (on the router's back panel).

Click "Apply" to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

3.1.3 Remote Management

This function allows you to designate a host on the Internet so he can configure the router from a remote site. Enter the designated host's IP address in the Host Address field.

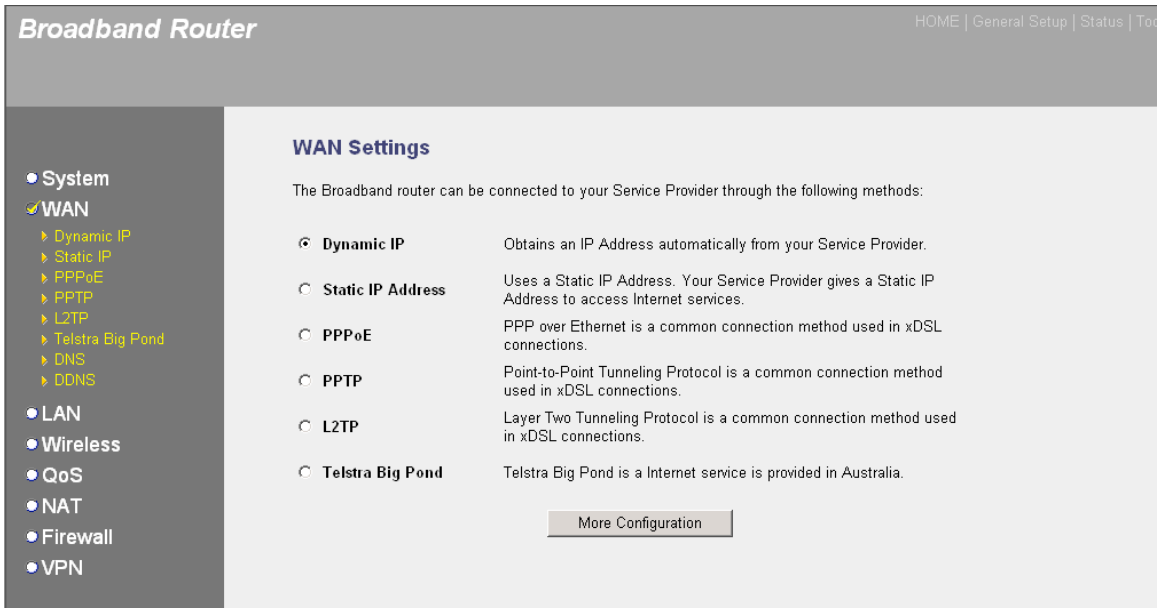


Parameter	Description
Host Address	This is the IP address of the host on the Internet that will have remote management/configuration access to the router. This means if you're at home and your home IP address has been designated the Remote Management host IP address for this router (located in your company office), then you're able to configure this router from your home. If the Host Address is left as 0.0.0.0, this means anyone can access the router's Web-based configuration from a remote location, provided they know the password. Click the "Enabled" box to enable the Remote Management function. ***Note:*** To access the Web-based management from a remote site, you must enter the router's WAN IP address (e.g., 10.0.0.1) into your Web browser, followed by port number 8080 (e.g., 10.0.0.1:8080), as shown below. You'll also need to know the password set on the Password Setting screen in order to access the router's Web-based management. 
Port	This is the port number of remote-management Web interface.
Enabled	Select to enable the Remote Management function.

Click "Apply" at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

3.2 WAN

Use the WAN Settings screen if you have already configured the Quick Setup Wizard section and you would like to change your Internet connection type: Dynamic IP, Static IP Address, PPPoE, PPTP, L2TP, Telstra BigPond, DNS and DDNS. Once you've made a selection, click "More Configuration" at the bottom of the screen and proceed to the manual's corresponding sub-section.



3.2.1 Dynamic IP

Select if your ISP will automatically give you an IP address. Some ISPs may also require that you fill in additional information, such as Host Name, Domain Name and MAC address (see Section 2.2.2 for more details).

3.2.2 Static IP Address

Select if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section. (see Section 2.2.2 for more details).

3.2.3 PPPoE (PPP over Ethernet)

Select if your ISP requires the PPPoE protocol to connect to the Internet. Your ISP should provide all the information required in this section. (see Section 2.2.2 for more details).

3.2.4 PPTP

Select if your ISP requires the PPTP protocol to connect to the Internet. Your ISP should provide all the information required in this section. (see Section 2.2.2 for more details).

3.2.5 L2TP

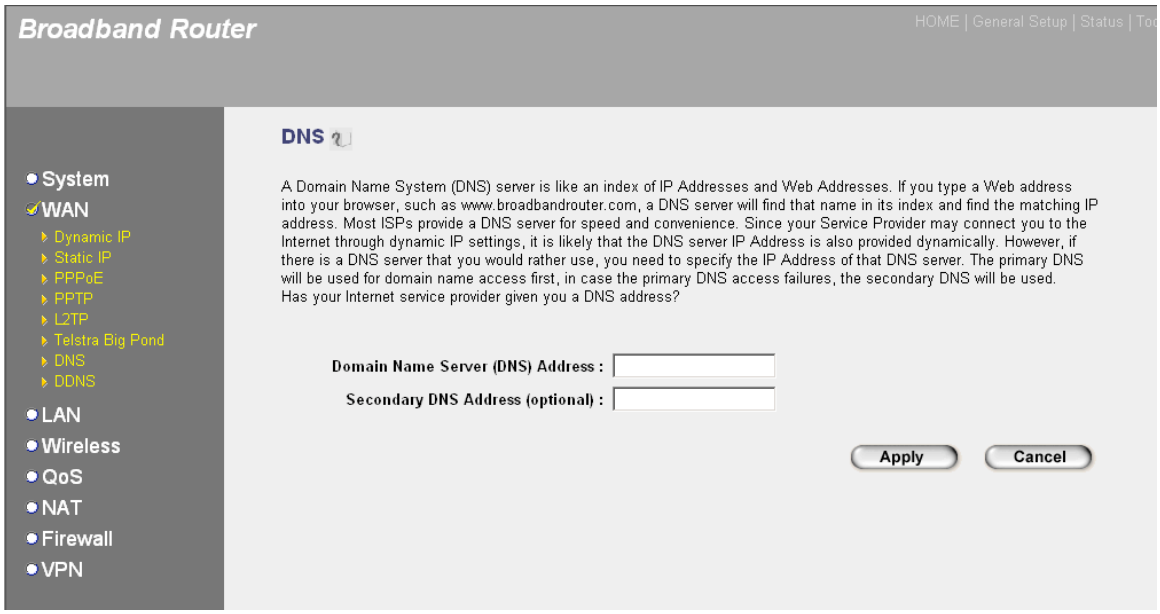
Select if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section. (see Section 2.2.2 for more details).

3.2.6 Telstra BigPond

Select if your ISP requires the Telstra BigPond protocol to connect you to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia. (see Section 2.2.2 for more details).

3.2.7 DNS

A Domain Name System (DNS) server is like an index of IP and Web addresses. If you type a Web address into your browser, such as www.router.com, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for speed and convenience. If your service provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather use, you need to specify its IP address here.

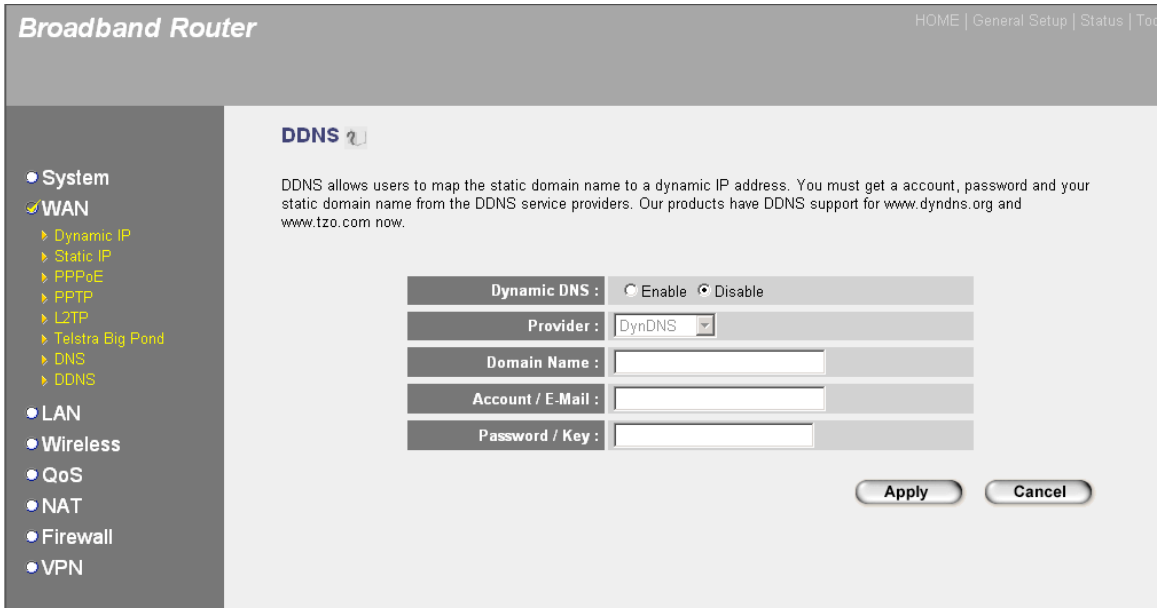


Parameter	Description
Domain Name Server (DNS) Server	This is the DNS server IP address that the ISP gave you; or you can specify your own preferred DNS server IP address.
Secondary DNS Address	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used should the above DNS fail.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

3.2.8 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.

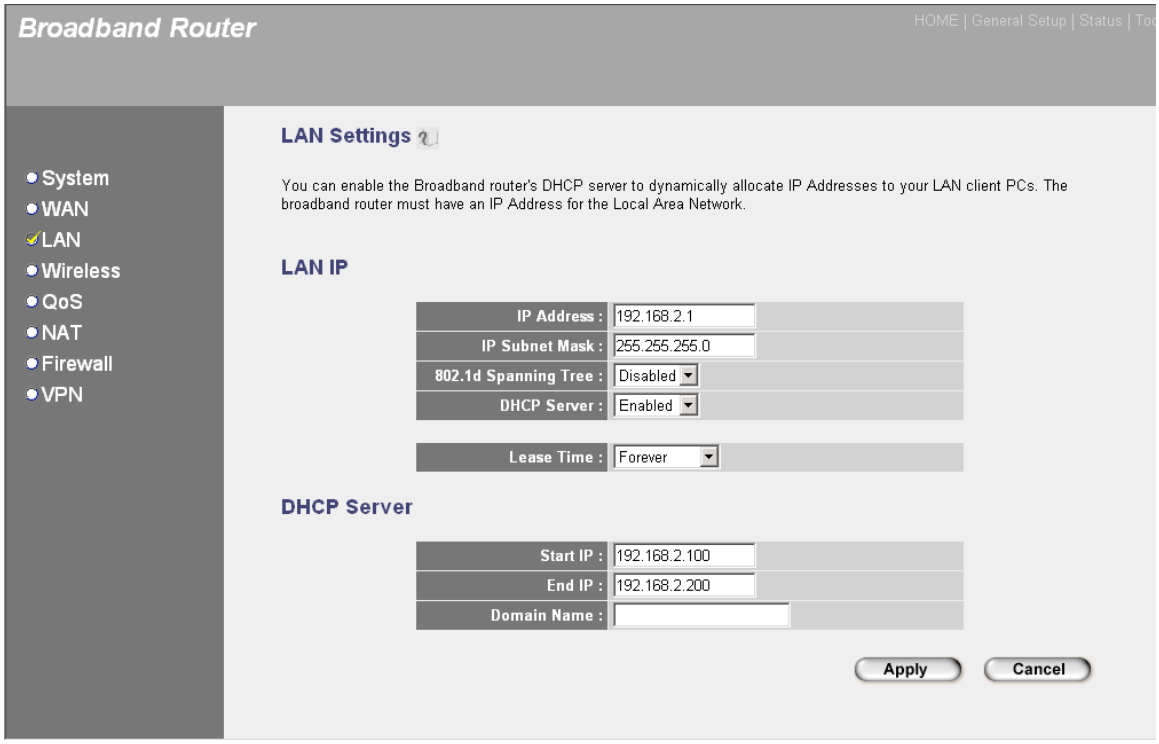


Parameter	Default	Description
Enable/Disable	Disable	Enable/Disable the DDNS function.
Provider		Select a DDNS service provider.
Domain Name		Your static domain name that uses DDNS.
Account/E-mail		The account that your DDNS service provider assigned to you.
Password/Key		The password you set for the DDNS service account above.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

3.3 LAN

Use this screen to specify a private IP address for your router's LAN ports (LAN IP panel), as well as a subnet mask for your LAN segment (DHCP Server panel).



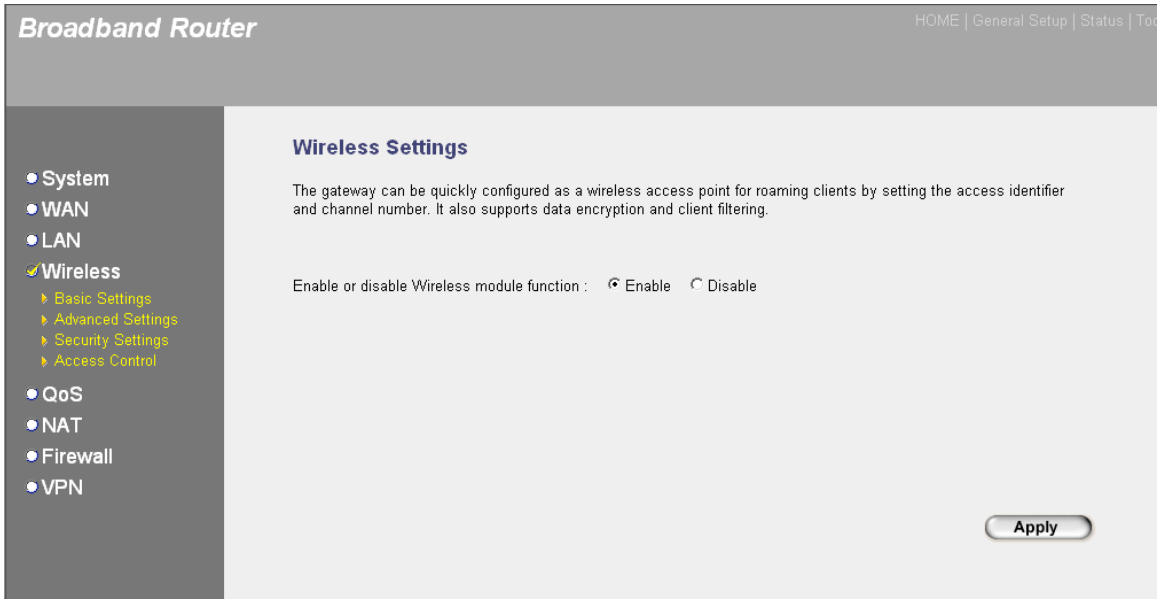
Parameter	Default	Description
IP Address	192.168.2.1	This is the router's LAN port IP address (your LAN clients' default gateway IP address).
IP Subnet Mask	255.255.255.0	Specify a subnet mask for your LAN segment.
802.1d Spanning Tree	Disabled	If this function is enabled, this router will use the spanning tree protocol to prevent network looping in the LAN ports.
DHCP Server	Enabled	When enabled, the router will automatically give your LAN clients an IP address. If the DHCP is not enabled, you'll need to manually set your LAN clients' IP addresses. Make sure the LAN client is in the same subnet as this router if you want the router to be your LAN clients' default gateway.
Lease Time		When the DHCP is enabled, it temporarily gives your LAN clients an IP address. From the drop-down menu, you can specify the time

	period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN clients' IP address when this time threshold period is reached.
Start IP / End IP	You can select a particular IP "address pool" for your DHCP server to issue IP addresses to your LAN clients. ***Note:*** By default, the range is 192.168.2.100 (Start IP) to 192.168.2.199 (End IP). If you want your PC to have a static/fixed IP address, you'll need to choose an address outside this IP address pool.
Domain Name	Specify a domain name for your LAN.

Click "Apply" at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

3.4 Wireless

Wireless Access Point builds a wireless LAN and lets all PCs equipped with an IEEE 802.11b or 801.11g wireless network adapter connect to your intranet. It supports WEP and WPA2 encryption to enhance the security of your wireless network.



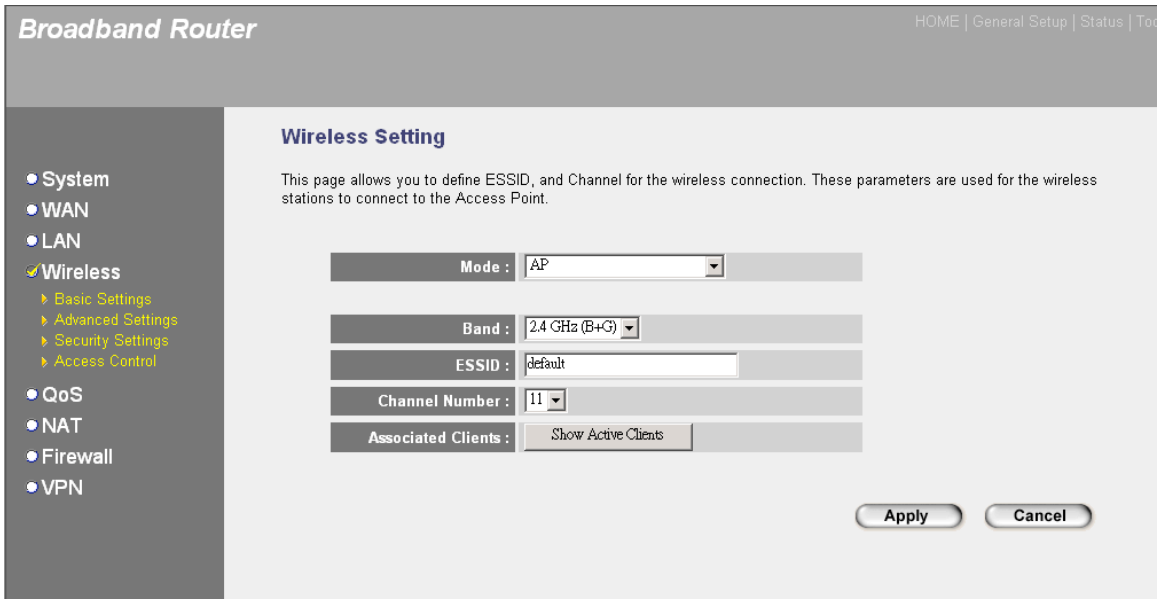
Parameter	Default	Description
Enable or disable	Enable	Enable or disable the wireless access point module of this router.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

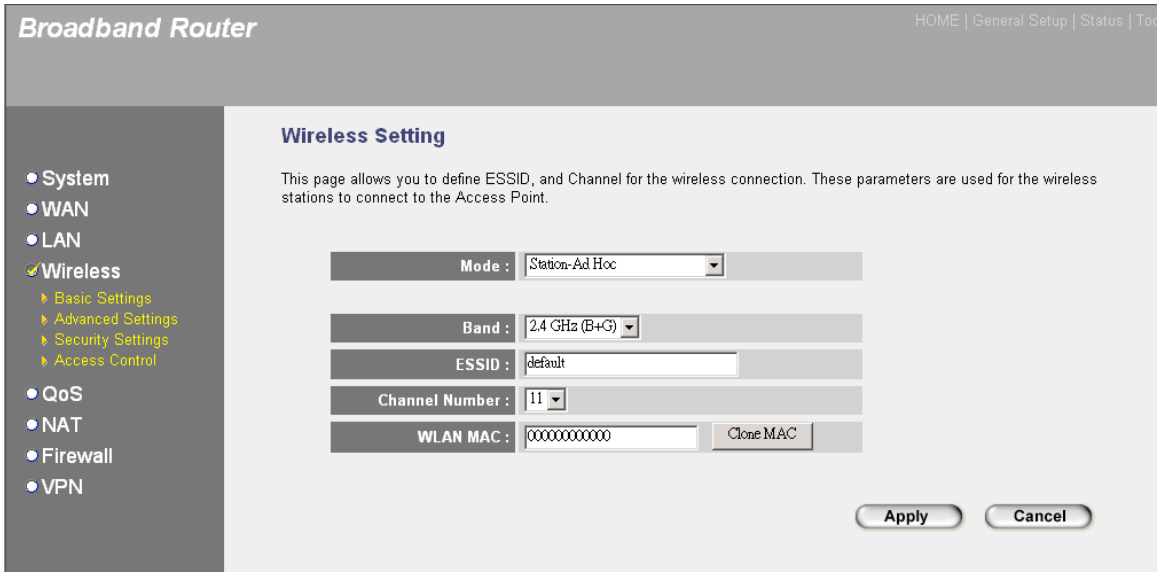
3.4.1 Basic Settings

Set the parameters that are used for the wireless stations to connect to this router. The screens for the six Mode options — “AP, “Station Ad-Hoc,” “Station Infrastructure,” “AP Bridge–Point to Point,” “AP Bridge–Point to Multi-Point” and “AP Bridge–WDS” — are presented below, with the common parameters described after the last screen.

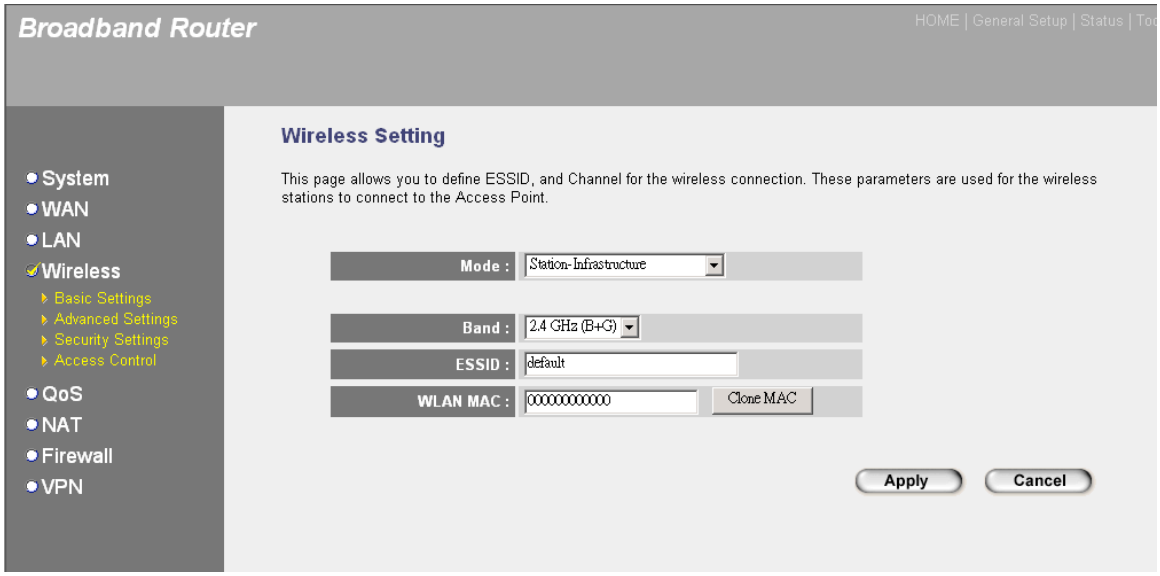
AP Mode:



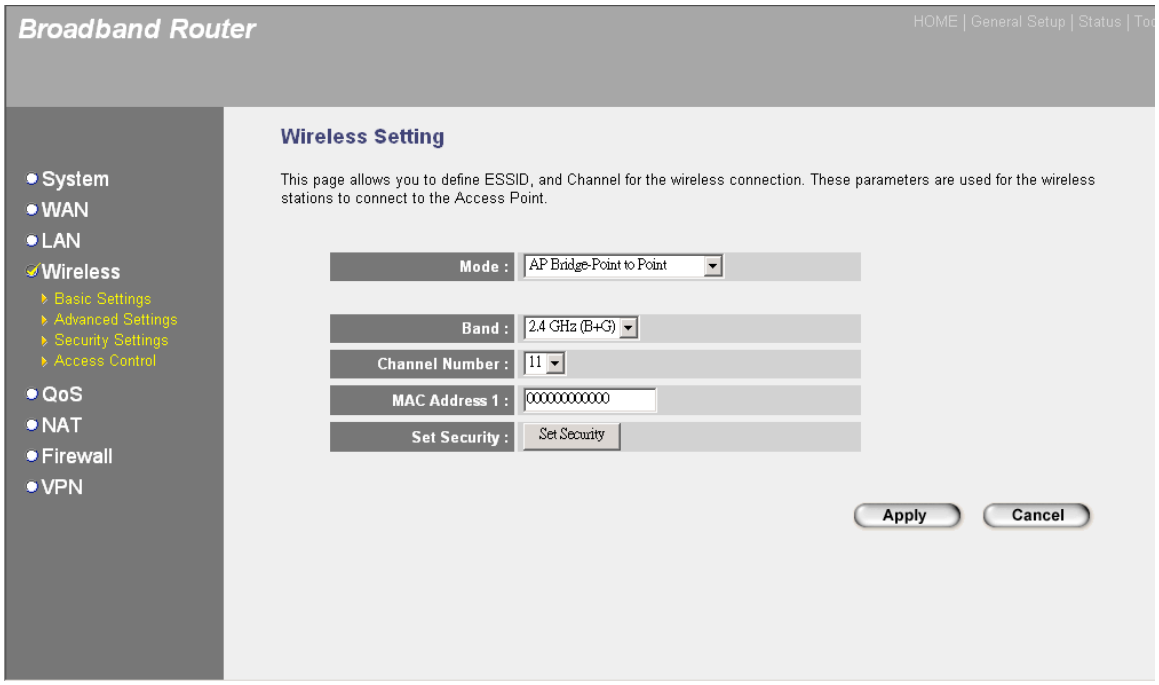
Station–Ad Hoc mode:



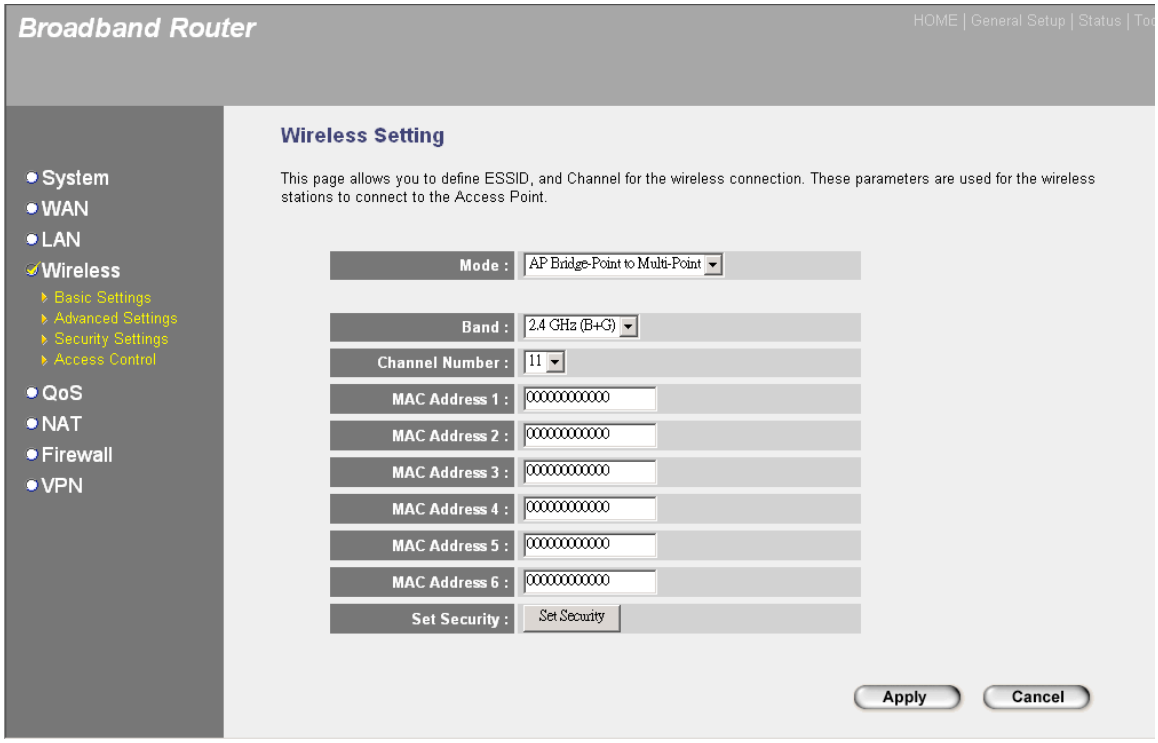
Station–Infrastructure mode:



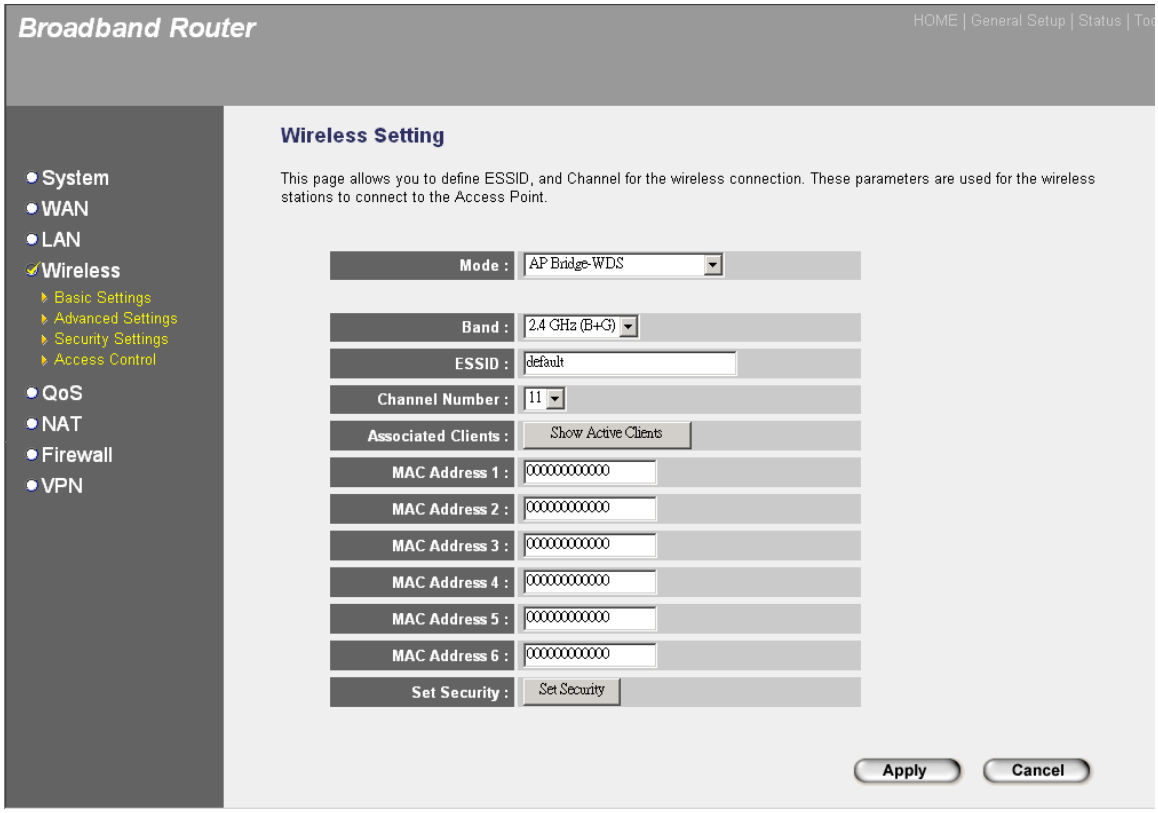
AP Bridge–Point to Point mode:



AP Bridge–Point to Multi-Point mode:



AP Bridge–WDS mode:

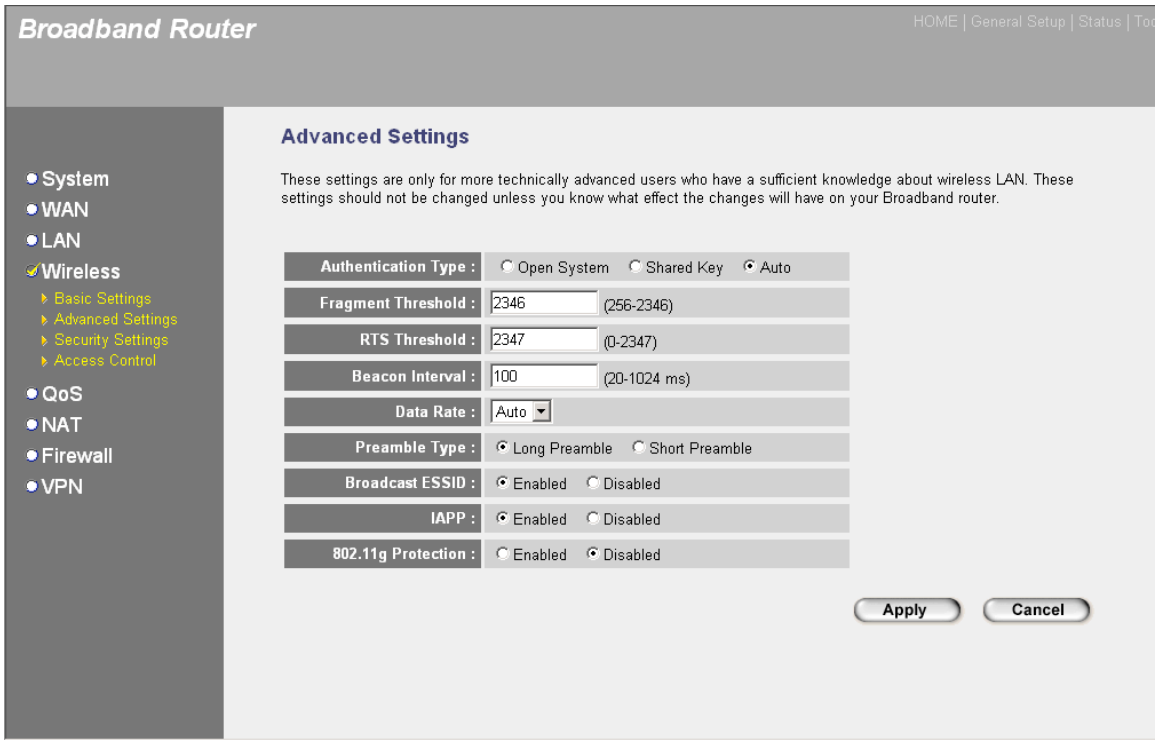


Parameter	Default	Description
Mode		Select one of the six modes shown above.
Band		Fix the AP at 802.11b or 802.11g mode, or select the B+G mode to allow the AP to select either 802.11b or 802.11g automatically.
ESSID	Default	This is the name of the wireless LAN. All the devices in the same wireless LAN should have the same ESSID.
Channel Number	11	This is the channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.
Associated Clients		Click “Show Active Clients” to display the Active Wireless Client table, which shows the status of all active wireless stations that are connecting to the access point.
WLAN MAC		This is the MAC address used by the wireless interface of this AP when it’s in a station mode.
Clone MAC		Click to copy the MAC address of your PC, which you’re using to configure the AP, to the WLAN MAC.
MAC address		To bridge more than one network together with the wireless LAN, set this access point to “AP Bridge–Point to Point,“ “AP Bridge–Point to Multi-Point” or “AP Bridge–WDS.” Then enter the MAC addresses of other access points that are joining the bridged network.
Set Security		Click to display the WDS Security Settings screen. Set the security parameters used to bridge access points together when your AP is in an AP Bridge mode (see Section 3.4.3).

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advanced settings in place).)

3.4.2 Advanced Settings

Among the advanced wireless LAN parameters you can set are Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval and Preamble Type. ***Note:*** You should not change these parameters unless you know what effect the changes will have on this router.



Parameter	Description
Authentication Type	There are two authentication options: "Open System" and "Shared Key." When you select "Open System," wireless stations can associate with this wireless router without WEP encryption. When you select "Shared Key," you should also set up WEP key on the Encryption screen and wireless stations should use WEP encryption in the authentication phase to associate with this wireless router. If you select "Auto," the wireless client can associate with this wireless router by using either of the authentication types.
Fragment Threshold	Specify the maximum size of packets during the fragmentation of data to be transmitted. ***Note:*** If you set this value too low, it will result in bad performance.

RTS Threshold	When the packet size is smaller the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	This is the interval of time that this wireless router broadcasts a beacon, which is used to synchronize the wireless network.
Data Rate	This is the rate this access point transmits data packets. The access point will use the highest possible selected transmission.
Preamble Type	“Long Preamble” can provide better wireless LAN Compatibility; “Short Preamble” can provide better wireless LAN performance.
Broadcast ESSID	By enabling Broadcast ESSID, every wireless station located within the coverage of this access point can discover this access point easily. If you’re building a public wireless network, enabling this feature is recommended. Disabling Broadcast ESSID can provide better security.
IAPP	Enabling IAPP will allow wireless station roaming between IAPP-enabled access points within the same wireless LAN.
802.11g Protection	Also called CTS Protection. Enabling this function is recommended, as it can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower.

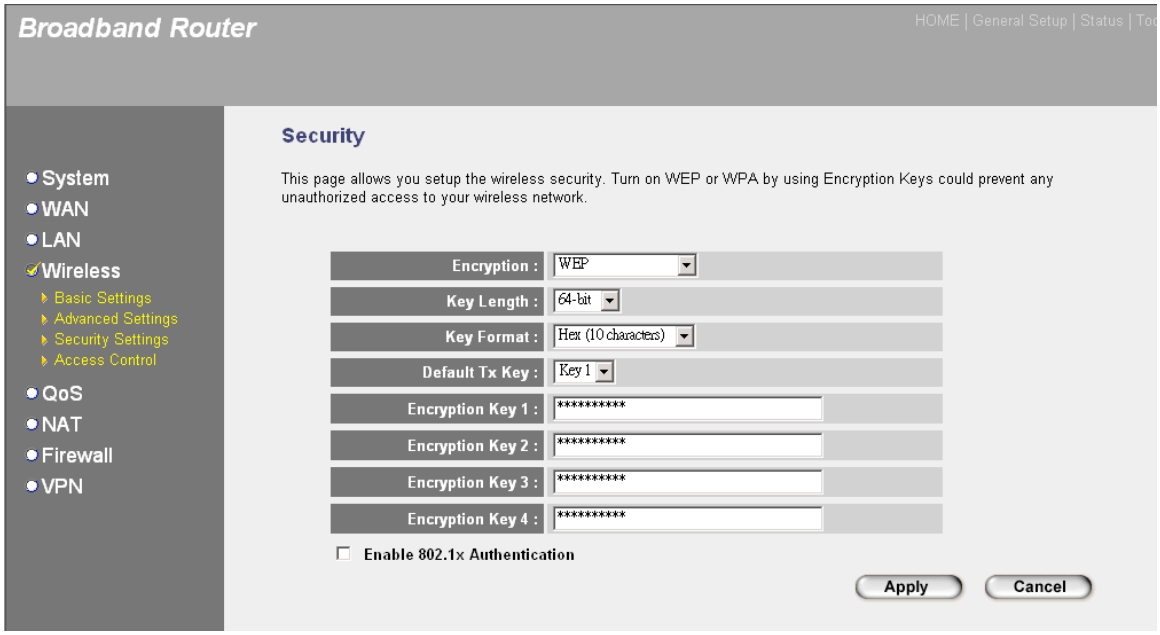
Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.4.3 Security

This Wireless G VPN Router provides complete wireless LAN security functions, include WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can protect your wireless LAN from illegal access. Just make sure your wireless stations use the same security function.

3.4.3.1 WEP Only

When you select 64-bit or 128-bit WEP key, you need to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can also enter four WEP keys and select one of them as a default key: Then the router can receive any packets encrypted by one of the four keys.

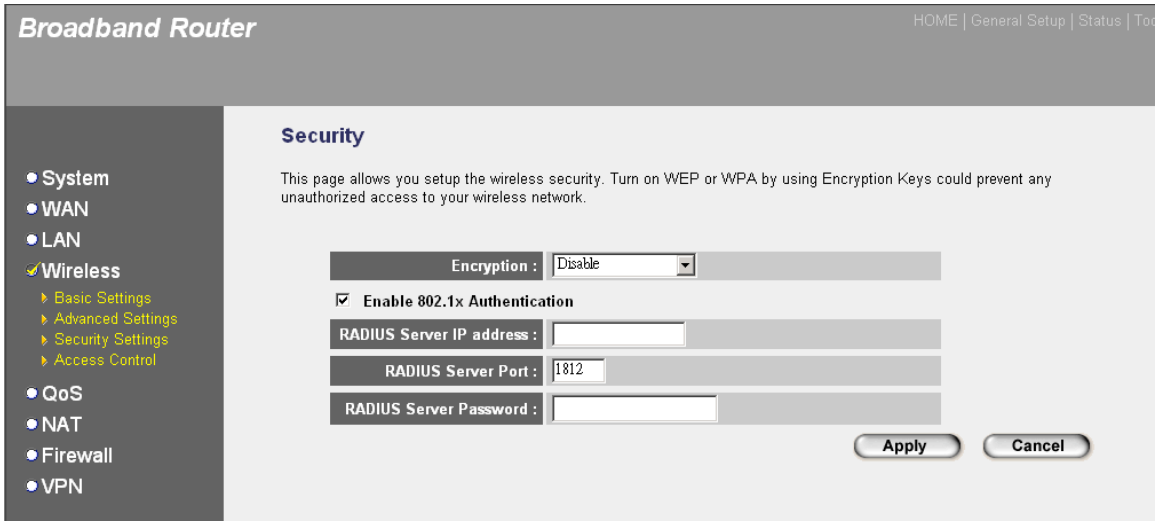


Parameter	Default	Description
Key Length	64-bit	Select “64-bit” or “128-bit.” The larger WEP key length will provide a higher level of security, but the throughput will be lower.
Key Format		You can use ASCII characters (alphanumeric format; e.g., “guest”) or hexadecimal digits (in the "A-F," a-f" and "0-9" ranges; e.g., 123abc) to be the WEP Key.
Default Key		Select one of the four keys to encrypt your data.
Key 1 - Key 4		The WEP keys are used to encrypt data transmitted in the wireless network. To place entries in the text fields: 64-bit WEP: Input 10-digit hex values (in the "A-F," "a-f" and "0-9" ranges) or 5-digit ASCII code as the encryption keys. 128-bit WEP: Input 26-digit hex values (in the "A-F," "a-f" and "0-9" ranges) or 13-digit ASCII codes as the encryption keys.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.4.3.2 802.1x Only

IEEE 802.1x is an authentication protocol. Every user must use a valid account to log in to this Wireless G VPN Router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates a user by IEEE 802.1x; it does not encrypt the data during communication.

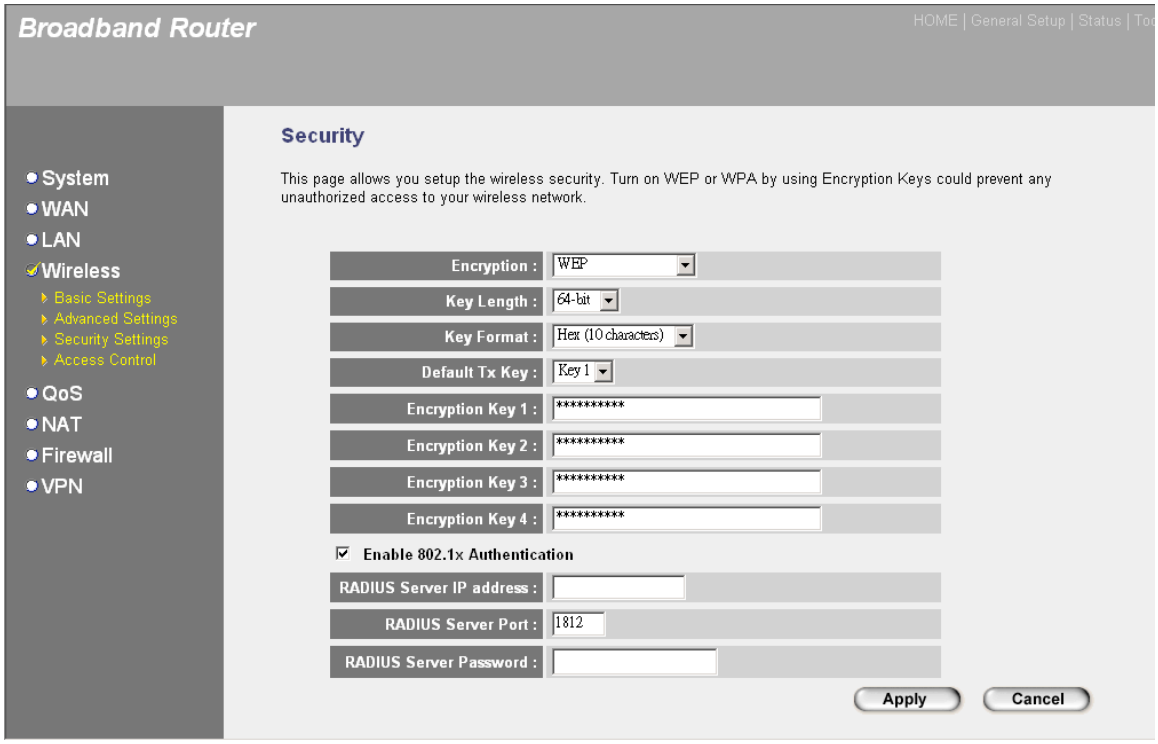


Parameter	Description
RADIUS Server IP Address	Enter the IP address of the external RADIUS server.
RADIUS Server Port	This is the service port of the external RADIUS server.
RADIUS Server Password	Enter the password used for the external RADIUS server.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.4.3.3 802.1x WEP Static Key

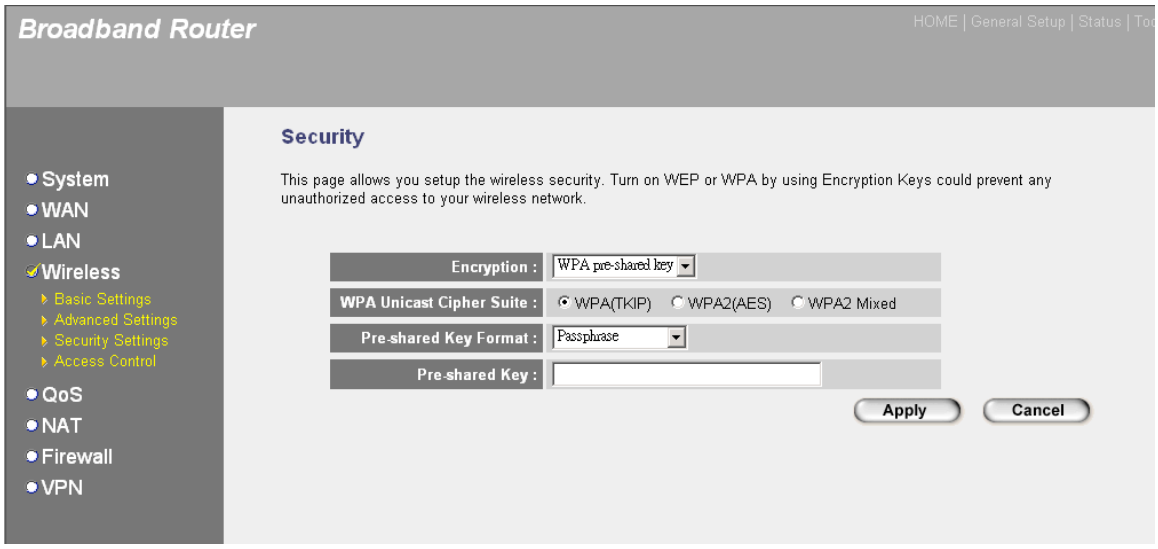
IEEE 802.1x is an authentication protocol. Every user must use a valid account to log in to this Wireless G VPN Router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode also uses WEP to encrypt the data during communication.



For the WEP settings, refer to Section 3.4.3.1 (WEP Only). For the 802.1x settings, refer to section 3.4.3.2 (802.1x Only).

3.4.3.4 WPA Pre-Shared Key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently so the encryption key can't easily be broken by hackers, which vastly improves your security.

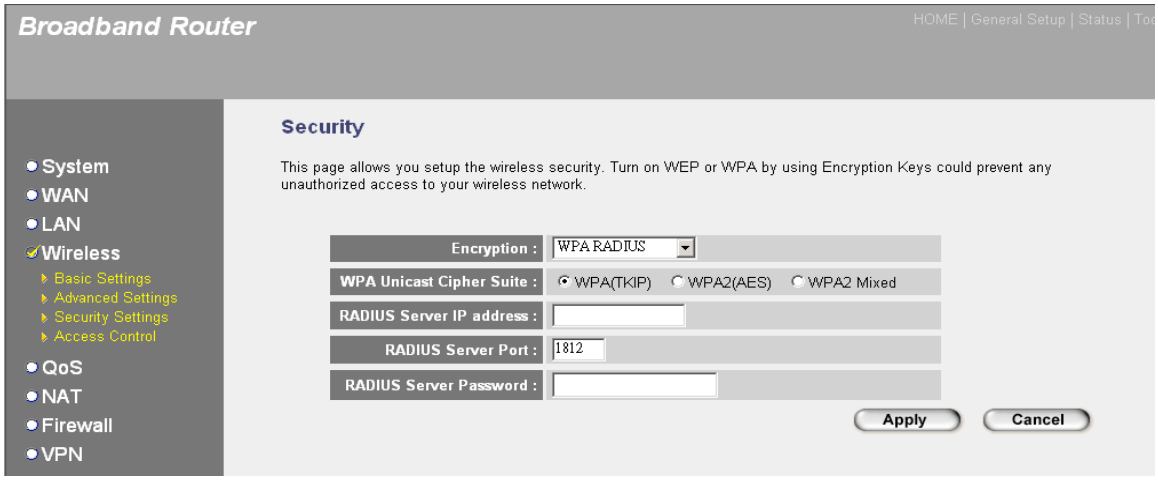


Parameter	Description
WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2 (AES)	This uses the CCMP protocol to change the encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
WPA2 Mixed	This will automatically use TKIP or AES based on the other communication peer.
Pre-Shared Key Format	Select “Passphrase” (alphanumeric format; e.g., “iamguest”) or “Hexadecimal Digits” (in the “A-F,” “a-f” and “0-9” ranges; “12345abcde”) for the format.
Pre-Shared Key	The pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. To place entries in the text fields: 64-bit WEP: Input 10-digit hex values (in the "A-F," "a-f" and "0-9" ranges) or 5-digit ASCII code as the encryption keys. 128-bit WEP: Input 26-digit hex values (in the "A-F," "a-f" and "0-9" ranges) or 13-digit ASCII codes as the encryption keys.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.4.3.5 WPA RADIUS

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently, which vastly improves your security.

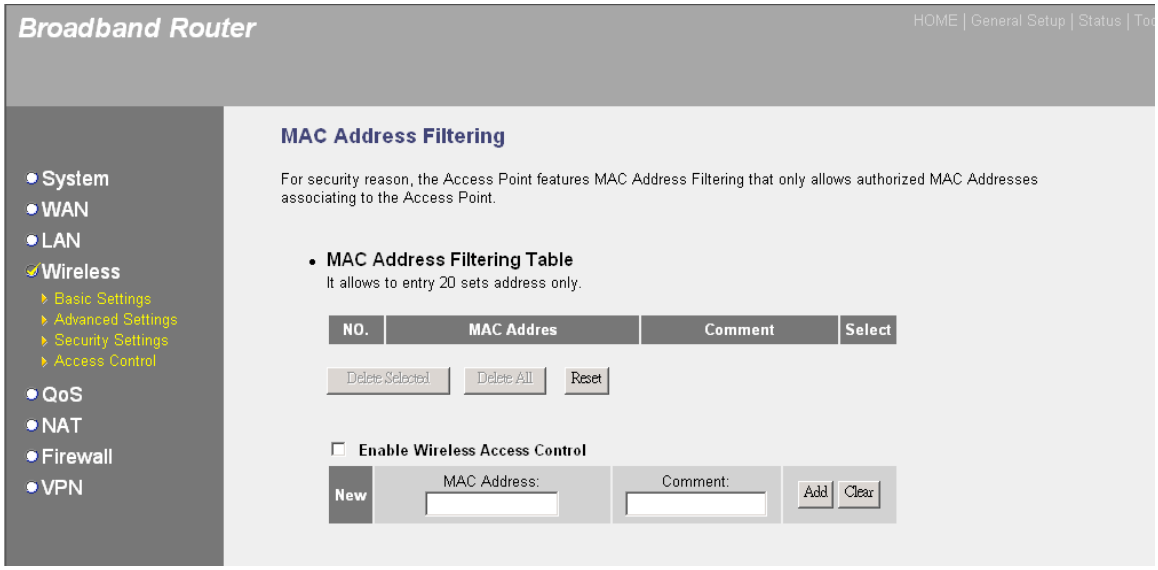


Parameter	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This uses the CCMP protocol to change the encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
WPA2 Mixed	This will automatically use TKIP or AES based on the other communication peer.
RADIUS Server IP Address	Enter the IP address of the external RADIUS server.
RADIUS Server Port	This is the service port of the external RADIUS server.
RADIUS Server Password	Enter the password used for the external RADIUS server.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.4.4 Access Control

These settings prevent unauthorized MAC addresses from accessing your wireless network.



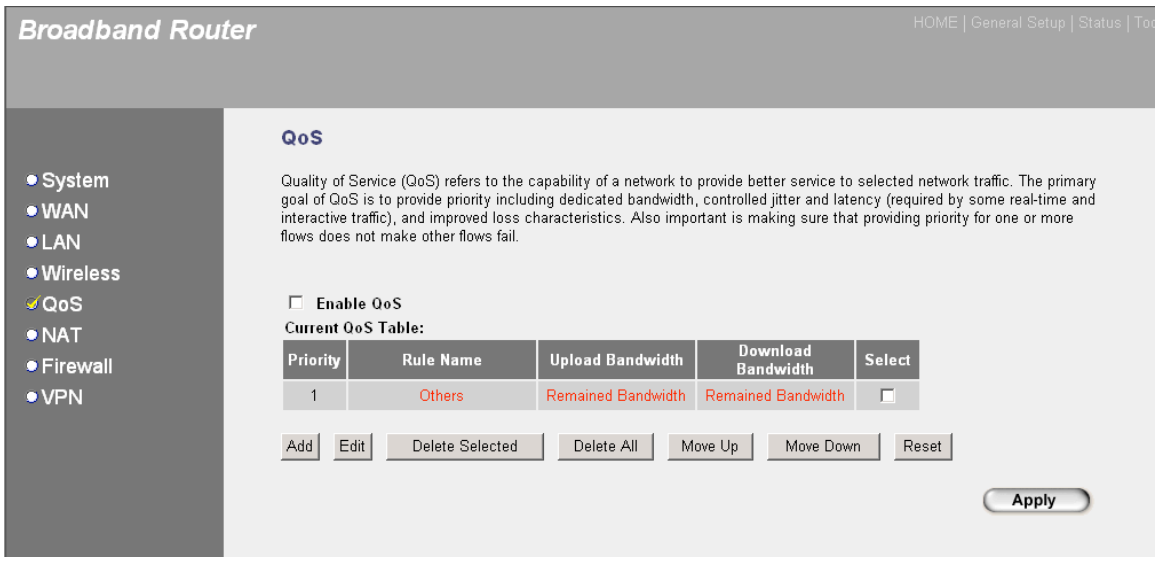
Parameter	Description
Enable wireless access control	Select to activate.

Add MAC address into the list	Fill in the "MAC Address" and "Comment" fields for the wireless station to be added and click "Add." This wireless station will then be added into the Current Access Control List that will display. Click "Clear" to empty both "MAC Address" and "Comment" fields if you need to re-enter text.
Remove MAC address from the list	To remove a MAC address from the Current Access Control List, select the MAC address(es) you want to remove in the list and click "Delete Selected." To remove all MAC addresses from the table, click "Delete All." Click "Reset" to clear current selections.

Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.5 QoS

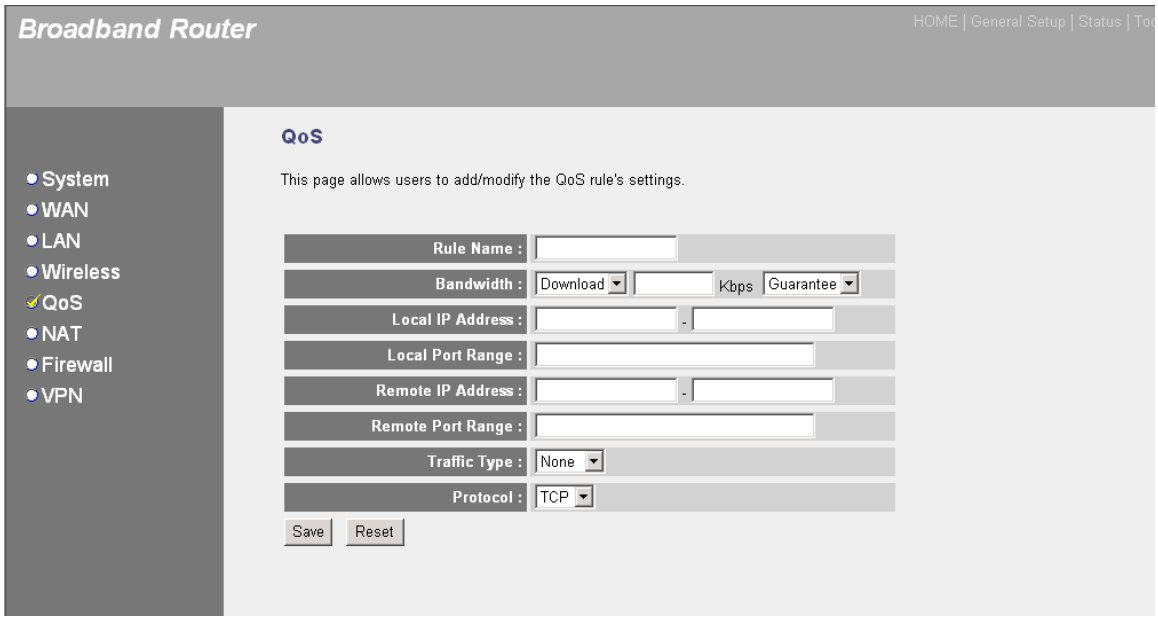
Quality of Service lets you classify Internet application traffic by source/ destination IP address and port number. You can assign a priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first: Lower-priority applications will get bandwidth after higher-priority applications get enough bandwidth. As a result, you enjoy a better experience when using critical real-time services such as Internet phone and video conferencing. All the applications not specified by you are classified as rule name “Others.” The rule with the smaller priority number has the higher priority; the rule with the larger priority number has the lower priority. You can adjust the priority of the rules by moving them up or down. ***Note:*** If the total assigned bandwidth of higher-priority applications is larger than the maximum bandwidth provided by the WAN port, the other applications will not get any bandwidth.



Parameter	Description
Enable/Disable QoS	Select to activate the QoS function for the WAN port. De-select to disable it.
Add a QoS rule into the table	Click “Add” to enter a form of the QoS rule. Click “Apply” after filling out the form and the rule will be added into the table.
Remove QoS rules from the table	To remove some QoS rules from the table, select the QoS rules you want to remove and click "Delete Selected." To remove all QoS rules from the table, click "Delete All." Click "Reset" to clear current selections.
Edit a QoS rule	Select the rule you want to edit and click “Edit.” Then enter the detail form of the QoS rule. Click “Apply” after editing the form and the rule will be saved.
Adjust QoS rule priority	Select the rule and click “Move Up” to make its priority Higher; select the rule and click “Move Down” to make its priority lower.

3.5.1 Edit QoS Rule

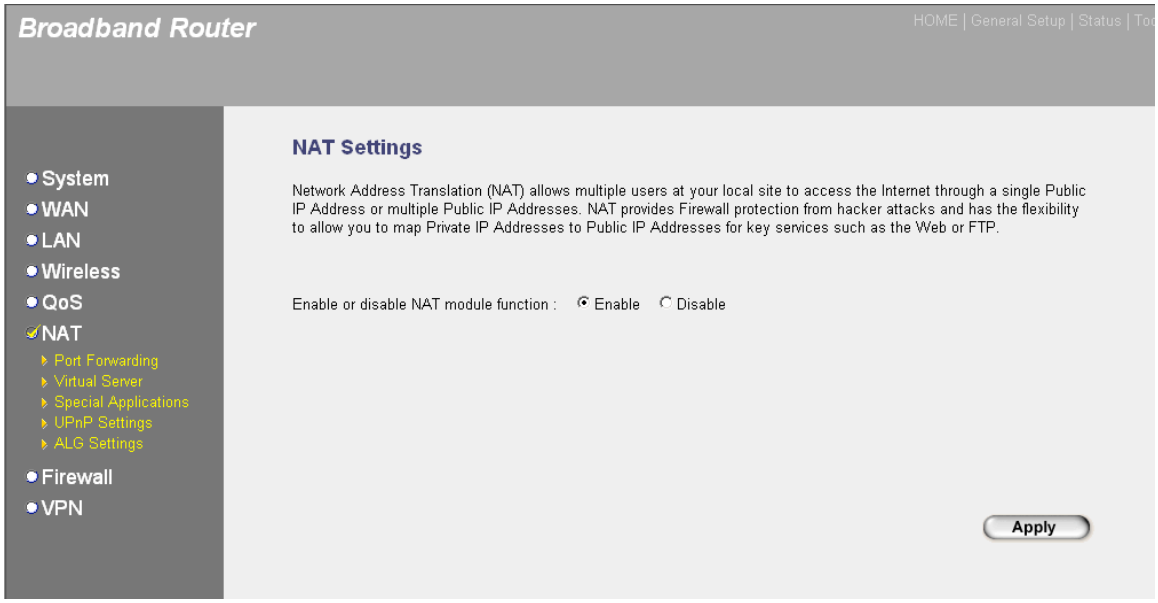
You can assign packet classification criteria by its local IP range, remote IP range, traffic type, protocol, local port range and remote port range parameters. The parameters that you leave blank will be ignored. The priority of this rule will be applied to packets that match classification criteria of this rule. You can limit bandwidth consumed by packets that match this rule or guarantee bandwidth required by packets that match this rule.



Parameter	Description
Rule Name	Enter a name for this rule.
Bandwidth	Select “Download” or “Upload” and assign a value (in Kbps). You can limit the maximum bandwidth consumed by this rule by selecting “Maximum.” You also can reserve enough bandwidth for this rule by selecting “Guarantee.”
Local IP Address	Enter the local IP address range of the packets this rule will apply to. If you assign 192.168.2.3 – 192.168.2.5, it affects three IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5
Local Port Range	Enter the local port range of the packets this rule will apply to. You can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a hyphen; for example, “101-150” means from port number 101 through port number 150 – a range of 50 ports.
Remote IP Address	Enter the remote IP address range of the packets this rule will apply to. If you assign 192.168.2.3 – 192.168.2.5, it affects three IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5
Remote Port Range	Enter the remote port range of the packets this rule will apply to. You can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a hyphen; for example, “101-150” means from port number 101 through port number 150 – a range of 50 ports.
Traffic Type	Select the traffic type of the packets this rule will apply to. Some popular applications are included in the menu, but you can get the same result by using other parameters (for example, source or destination port number) if you’re familiar with the application protocol.
Protocol	Select the protocol type of the packets this rule will apply to.
Save	Click to apply the settings and exit the form.
Reset	Click to clear the content of this form.

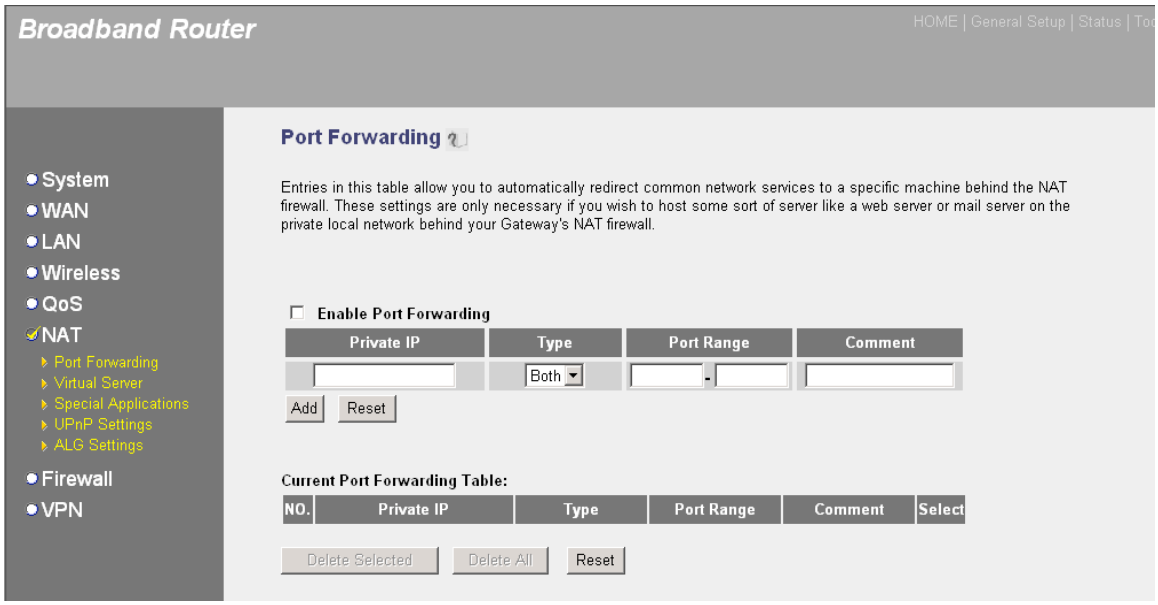
3.6 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT provides firewall protection from hacker attacks and has the flexibility to allow you to map private IP addresses to public IP addresses for key services such as Web sites and FTP sites.



3.6.1 Port Forwarding

This allows you to re-direct a particular range of service port numbers (from the Internet/WAN ports) to a particular LAN IP address. It also helps you host some servers behind the router's NAT firewall.

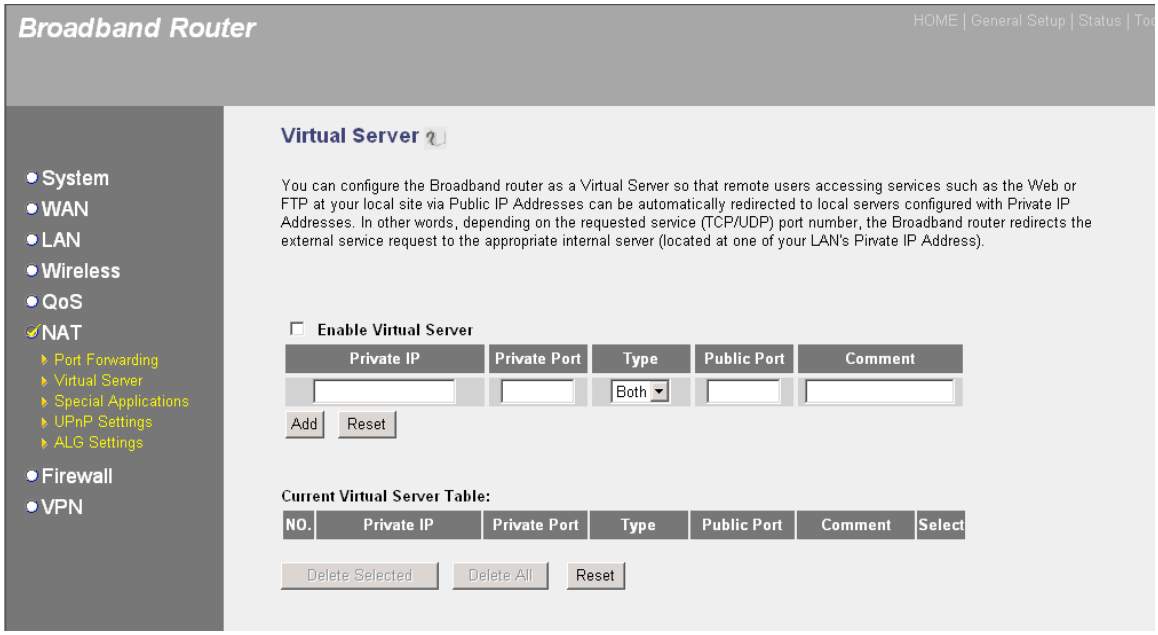


Parameter	Description
Enable Port Forwarding	Select to activate the function.
Private IP	This is the private IP of the server behind the NAT firewall. ***Note:*** You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
Type	This is the protocol type to be forwarded. You can choose to forward “TCP” or “UDP” packets only or select “Both” to forward both “TCP” and “UDP” packets.
Port Range	Enter the range of ports to be forwarded to the private IP.
Comment	Enter a description of this setting, if desired.
Add Port Forwarding into the table	Fill in the "Private IP," “Type,” “Port Range” and "Comment" fields of the setting to be added and click "Add." This Port Forwarding setting will then be added to the Current Port Forwarding Table below. To change or correct an entry before adding it, click "Clear" and re-enter.
Remove Port Forwarding from the table	Select the Port Forwarding settings you want to remove from the Current Port Forwarding table and click "Delete Selected." To remove all Port Forwarding settings from the table, click "Delete All." Click "Reset" to clear your current selections.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.6.2 Virtual Server

Use this function when you want different servers/clients in your LAN to handle different service/Internet application types (e.g., e-mail, FTP, Web server) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN port) to a particular LAN private IP address and its service port number.

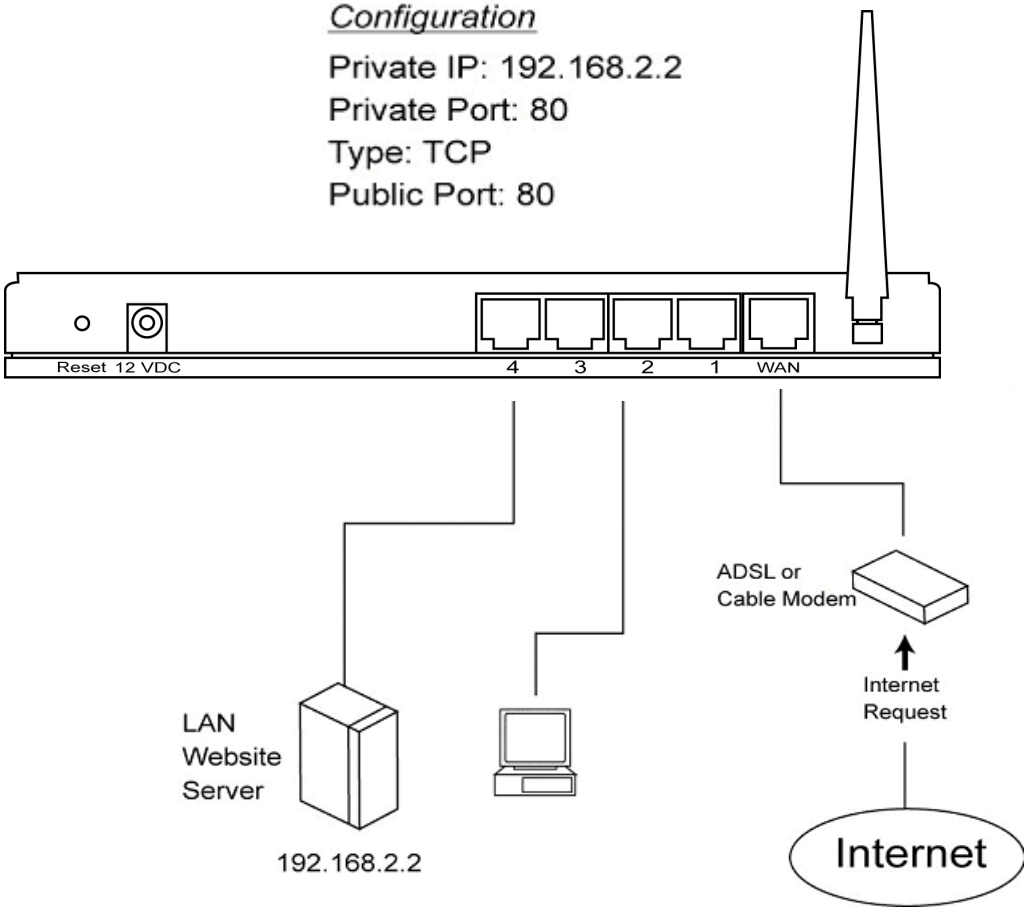


Parameter	Description
Enable Virtual Server	Select to activate the function.
Private IP	This is the LAN client/host IP address that the public port number packet will be sent to. ***Note:*** You need to give your LAN PC clients a fixed/static IP address for the virtual server to work properly.
Private Port	This is the port number (of the above private IP host) that the public port number (below) will be changed to when the packet enters your LAN (to the LAN Server/ Client IP).
Type	Select the port number protocol type (“TCP,” “UDP” or “Both”). If unsure, leave it to the default “Both.”
Public Port	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above private IP address host in your LAN. ***Note:*** The Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings.
Comment	Enter a description of this setting, if desired.
Add Virtual Server	Fill in the "Private IP," “Private Port,” “Type,” “Public Port” and "Comment" fields of the setting to be added and click "Add." This Virtual Server setting will then be

	added to the Current Virtual Server Table below. To change or correct an entry before adding it, click "Clear" and re-enter.
Remove Virtual Server	Select the Virtual Server settings you want to remove from the Current Virtual Server table and click "Delete Selected." To remove all Virtual Server settings from the table, click "Delete All." Click "Reset" to clear your current selections.

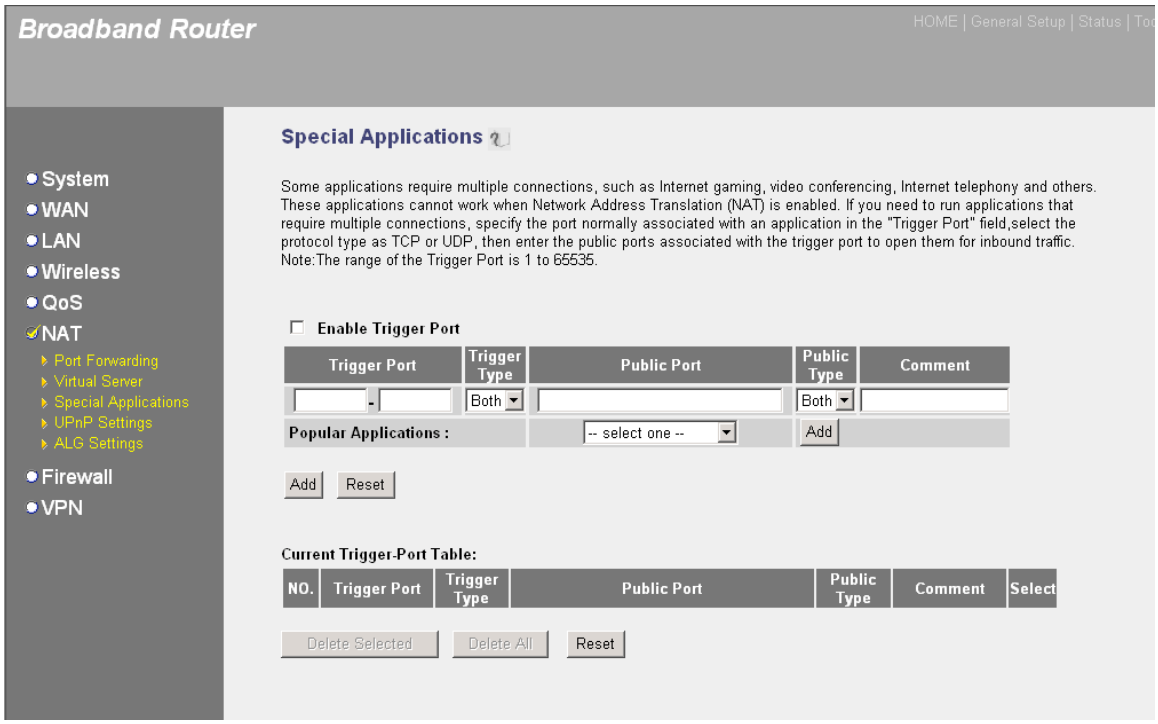
Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

Example of a Virtual Server:
The diagram below demonstrates one of the ways you can use the Virtual Server function. Use the virtual s when you want the Web server located in your private LAN to be accessible to Internet users. The configuration below means that any request coming from the Internet to access your Web server will be translated to your LAN’s Web server (192.168.2.2). ***Note:*** For the virtual server to work properly, Internet/remote users must know your global IP address. (For Web sites, you will need to have a fixed/static global/public IP address.)



3.6.3 Special Applications

Some applications — such as Internet games, video conferencing and Internet telephone — require multiple connections. On this screen, you can configure the router to support multiple connections for these types of applications.



Parameter	Description
Enable Trigger Port	Select to activate the function.
Trigger Port	This is the outgoing (outbound) range of port numbers for this particular application.
Trigger Type	Select whether the outbound port protocol is “TCP,” “UDP” or “Both.”
Public Port	Enter the incoming (inbound) port or port range for this type of application (e.g., 2300-2400, 47624). ***Note:*** Individual port numbers are separated by a comma (e.g., 47624, 5775, 6541). To input a port range, use a hyphen to separate the two port number ranges (e.g., 2300-2400).
Public Type	Select the inbound port protocol type: “TCP,” “UDP” or “Both.”
Comment	Enter a description of this setting, if desired.
Popular Applications	This section lists the more popular applications that

	require multiple connections. Select an application from the list, select a location (1-10) in the “Copy to” selection box, then click “Copy to.” This automatically lists the public ports required for this popular application in the location (1-10) you’ve specified.
Add Special Application	Fill in the "Trigger Port," "Trigger Type,” “Public Port,” "Public Type," "Public Port" and "Comment" fields of the setting to be added and click "Add.” This Special Application setting will be added to the Current Trigger-Port Table below. To change or correct an entry before adding it, click "Clear" and re-enter.
Remove Special Application	To remove a Special Application setting from the Current Trigger-Port Table, select the setting in the table and click "Delete Selected." To remove all settings from the table, click "Delete All." Click "Reset" to clear your current selections.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

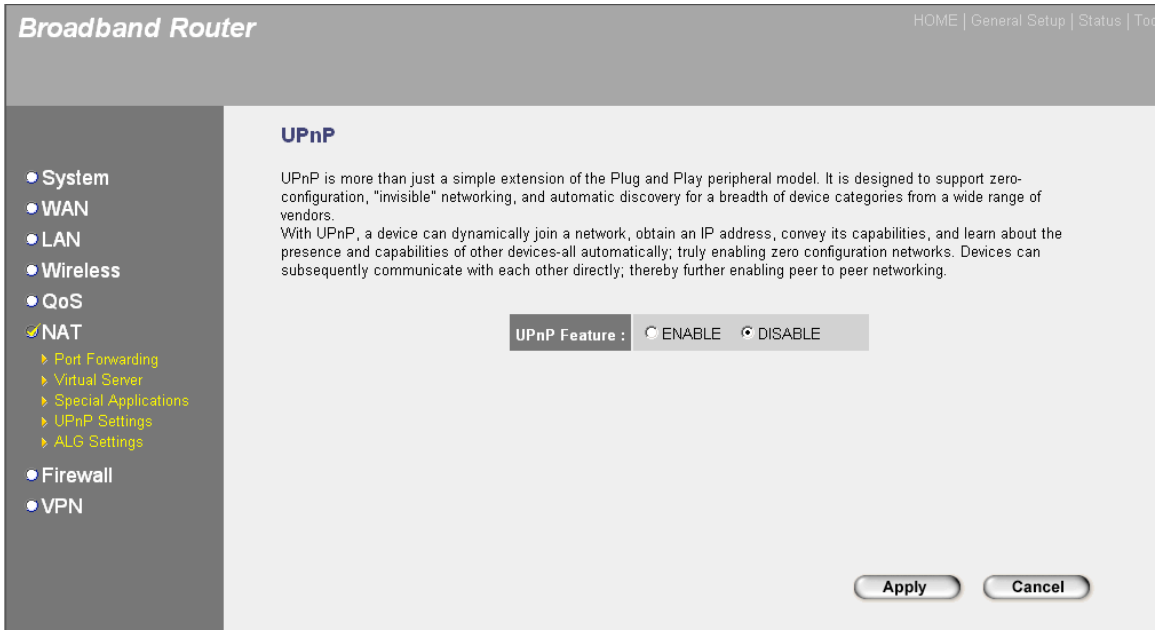
Example of Special Applications:
If you need to run applications that require multiple connections, specify the port (outbound) normally associated with that application in the "Trigger Port" field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

In the example above, when a user triggers port 28800 (outbound) for MSN Game Zone, the router will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user. ***Note:*** Only one LAN client can use a particular special application at a time.

3.6.4 UPnP

With UPnP, all PCs in you intranet will discover this router automatically: You do not need to do any configuration for your PC and can access the Internet through this router easily.

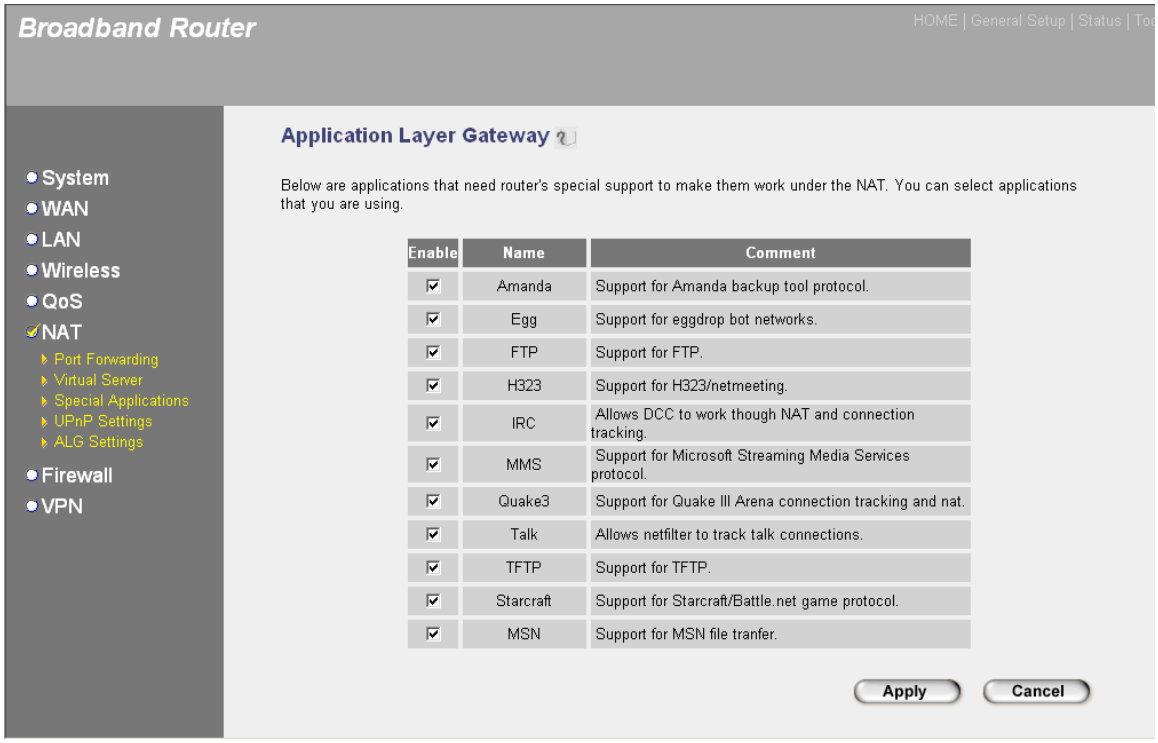


Parameter	Description
UPnP Feature	Select “Enable” or “Disable” (the default is “Disable”). After you enable the feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can allow applications that support UPnP smoothly connect to Internet sites without any incompatibility problem due to the NAPT port translation.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.6.5 ALG

You can select applications that need Application Layer Gateway for support.

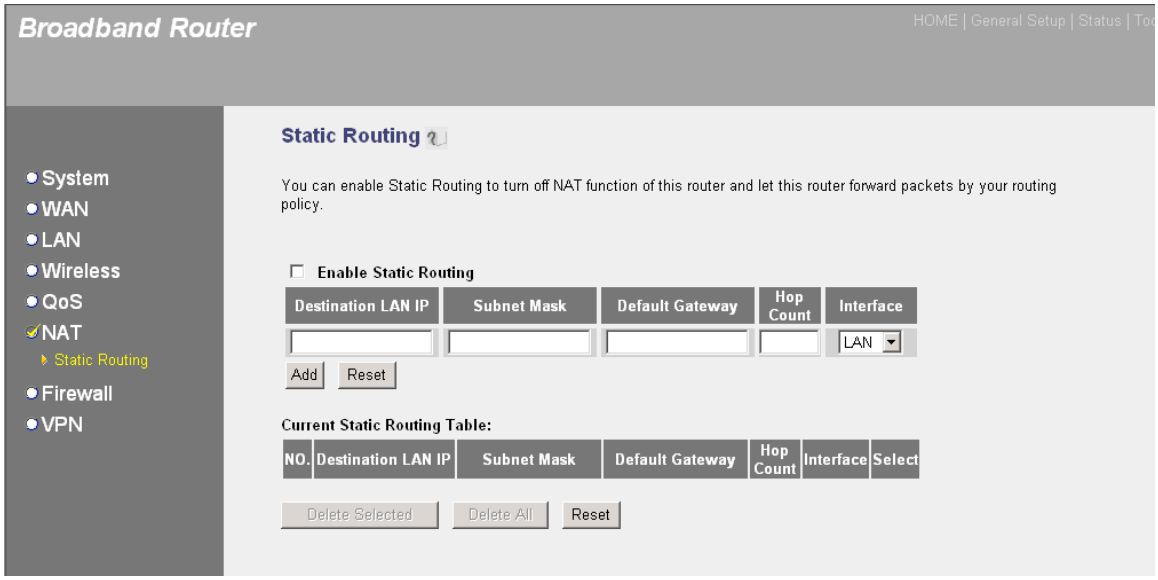


Parameter	Description
Enable	Select to enable Application Layer Gateway for any of the listed items. The router will then let that application correctly pass through the NAT gateway.

Click “Apply” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.6.6 Static Routing

This router makes the Static Routing function available when NAT is disabled. With Static Routing, the router can forward packets according to your routing rules. ***Note:*** The IP sharing function and the DMZ function of the firewall will not work in Static Routing mode.

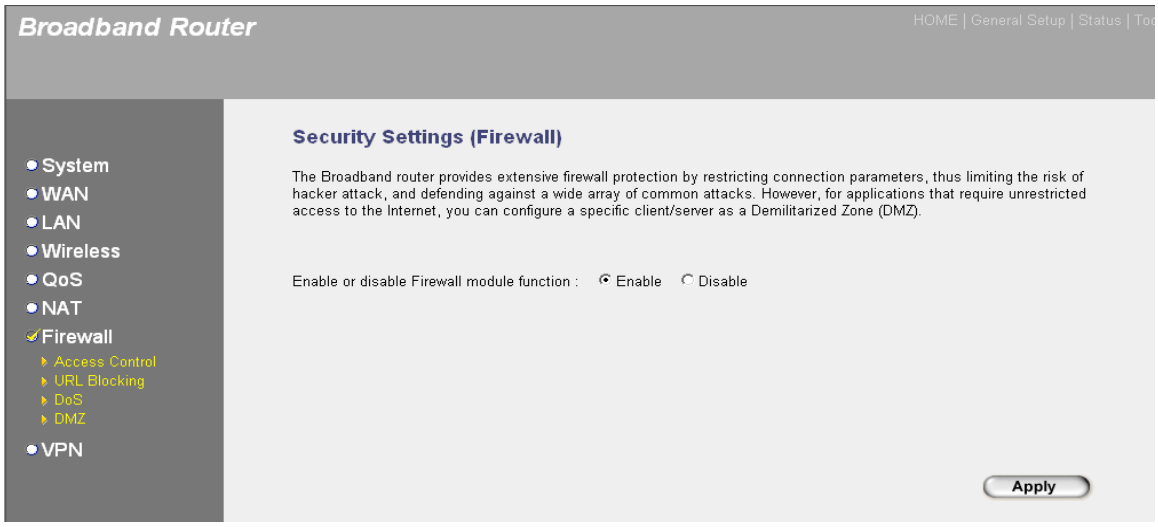


Parameter	Description
Enable Static Routing	Select to enable the function (it's disabled by default).
Destination LAN IP	Enter the network address of the destination LAN.
Subnet Mask	Enter the subnet mask of the destination LAN.
Default Gateway	Enter the next stop gateway of the path toward the destination LAN. This is the IP of the neighbor router that this router should communicate with on the path to the destination LAN.
Hop Count	Enter the number of hops (routers) to pass through to reach the destination LAN.
Interface	Select the interface that goes to the next hop (router).
Add a Rule	Fill in the "Destination LAN IP," "Subnet Mask," "Default Gateway," "Hop Count" and "Interface" of the rule to be added and click "Add." This rule will then be added into the Static Routing Table below. To change or correct an entry before adding it, click "Reset" to clear the fields, then re-enter.
Remove a Rule	To remove some routing rules from the Static Routing Table, select the rules in the table and click "Delete Selected." To remove all rules from the table, click "Delete All." Click "Reset" to clear current selections.

Click "Apply" at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

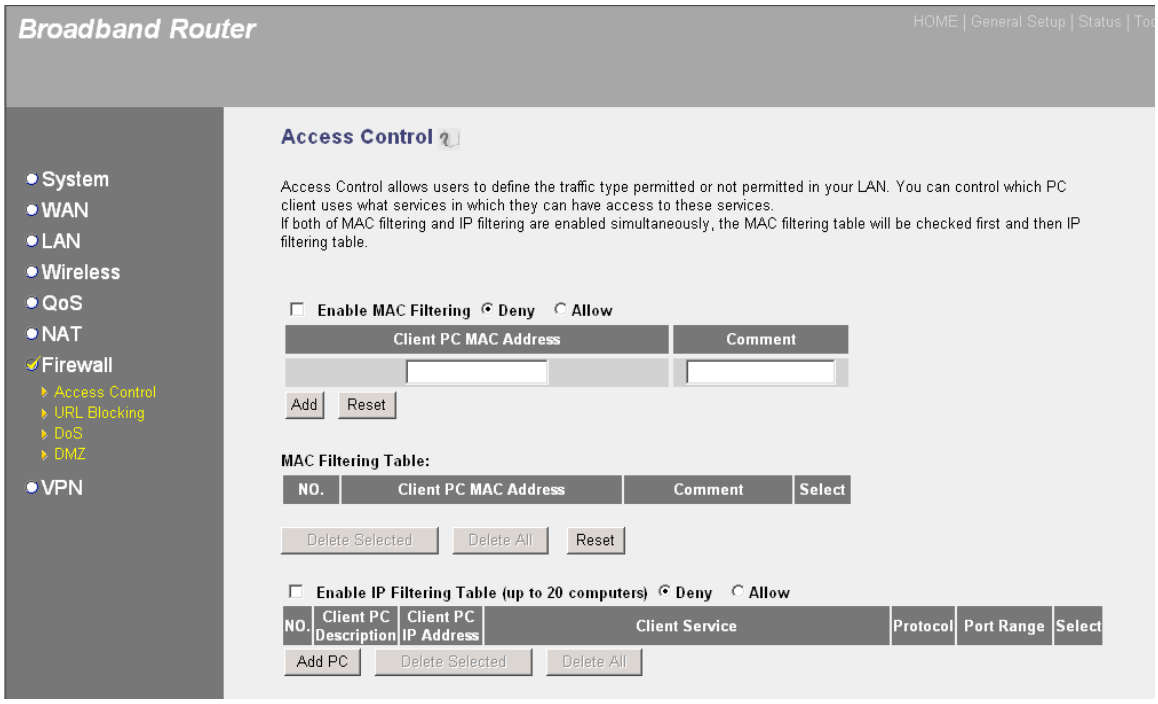
3.7 Firewall

This router provides extensive firewall protection by restricting connection parameters, thus limiting hacker attacks and defending against common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ). ***Note:*** To enable the Firewall settings, select “Enable” and click “Apply.”



3.7.1 Access Control

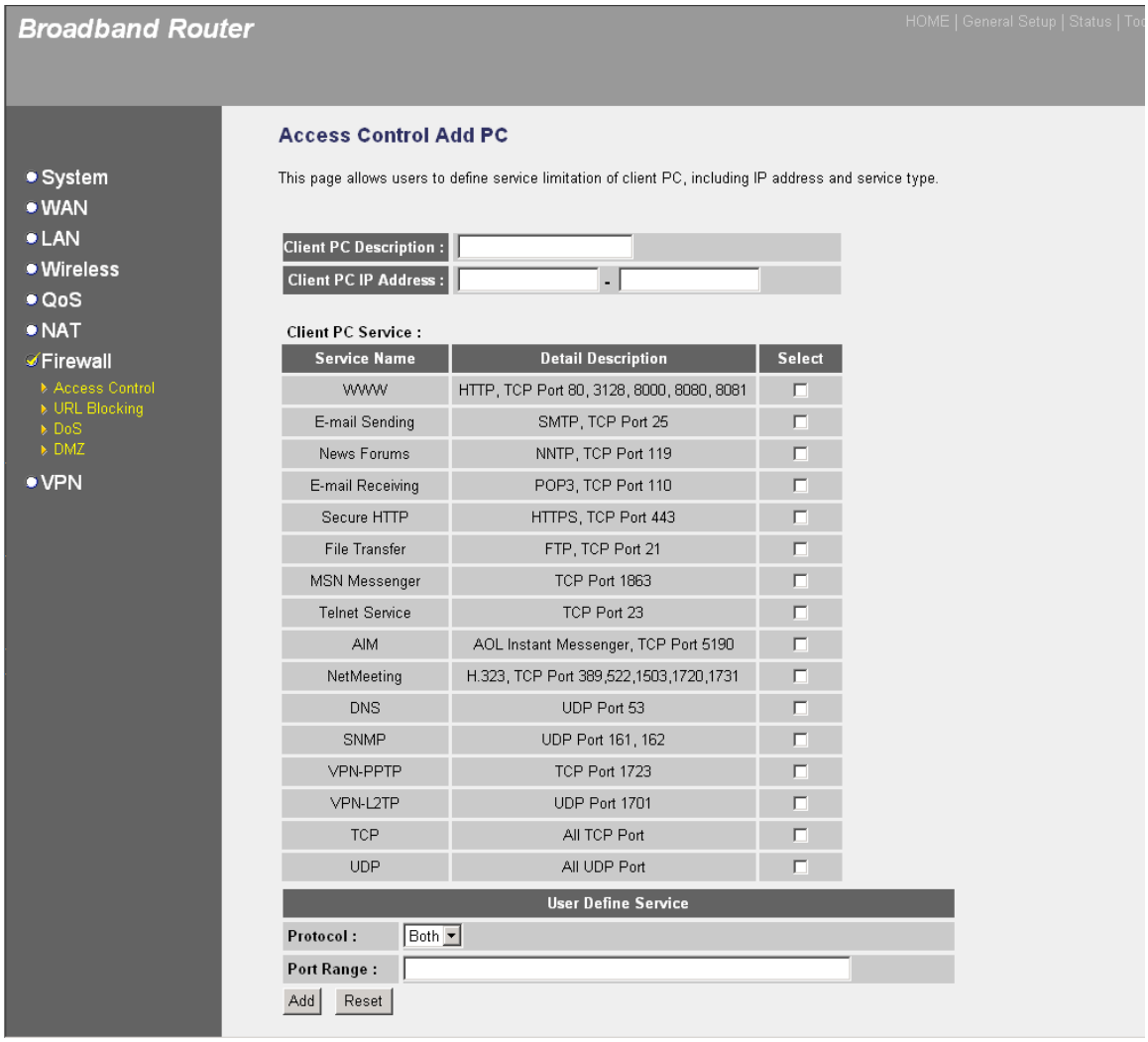
Access Control allows you to define the traffic type permitted in your LAN and restrict users from accessing certain Internet applications/services. You can control which PC client can have access to these services.



Parameter	Description
Enable MAC Filtering	Select to filter client PCs by MAC addresses.
Deny	Select for all PCs to be allowed Internet access, except for the PCs in the table below.
Allow	Select for all PCs to be denied Internet access, except for the PCs in the table below.
Add PC	Fill in the “Client PC MAC Address” and “Comment” fields of the PC that is allowed to access the Internet, then click “Add.” To change or correct an entry before adding it, click "Reset" to clear the fields, then re-enter.
Remove PC	To remove a PC from the MAC Filtering Table, select it and click "Delete Selected." To remove all PCs from the table, click "Delete All." To clear the selection and re-select, click “Reset.”
Enable IP Filtering Table	Select to filter client PCs by IP addresses.
Deny	Select for all PCs to be allowed Internet access, except for the PCs in the table below.
Allow	Select for all PCs to be denied Internet access, except for the PCs in the table below.
Add PC	Click to add an access control rule for users by IP addresses.
Remove PC	To remove a PC from the IP Filtering Table, select it in the table and click "Delete Selected." To remove all PCs from the table, click "Delete All."

You can now configure other sections or start using the router.

Access Control Add PC:

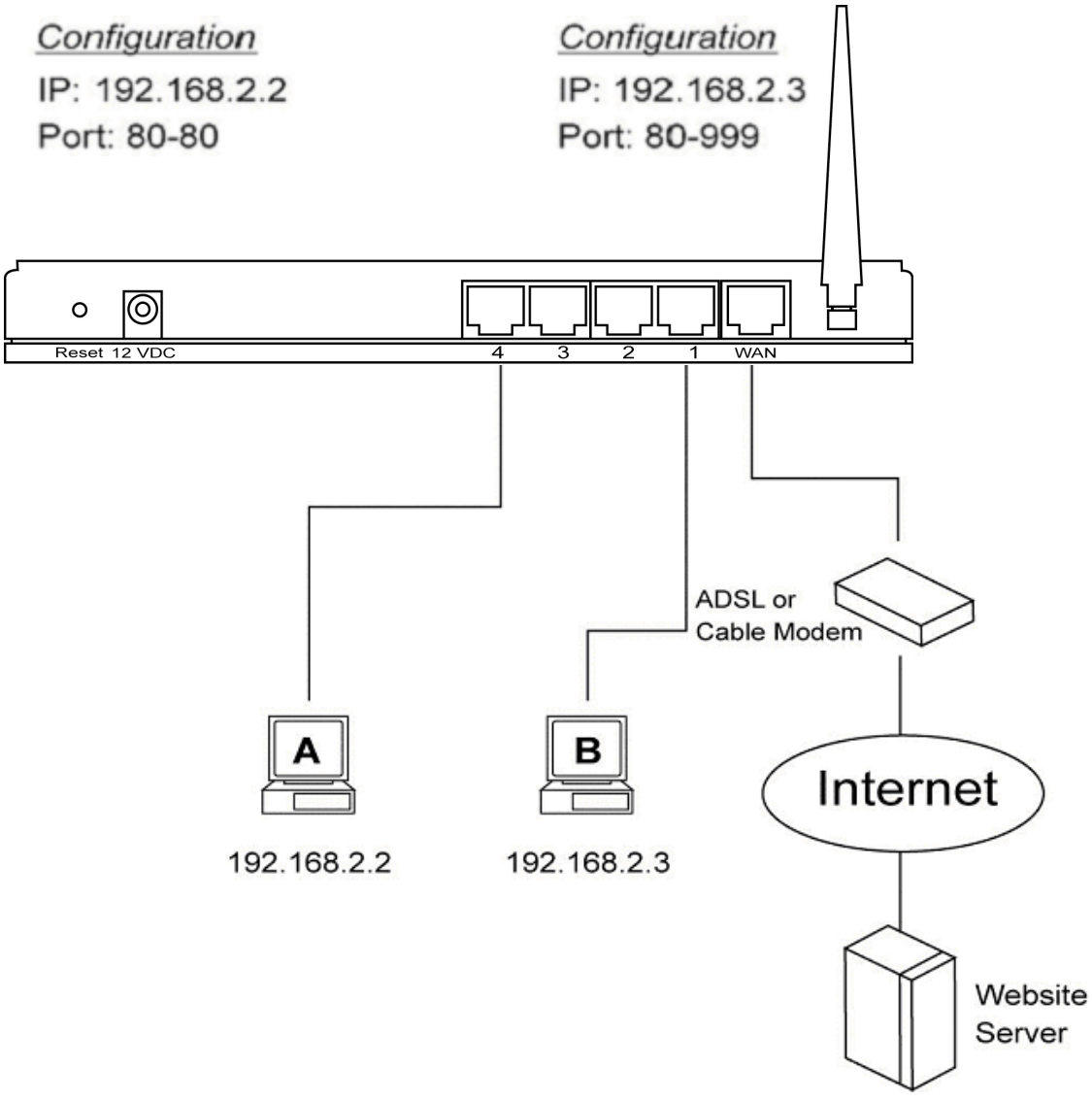


Parameter	Description
Client PC Description	Enter a description for this client PC rule, if desired.
Client PC IP Addresses	Enter the IP address range you want to apply to this Access Control rule. This is the user's IP address(es) that you want to set up an Access Control rule for. ***Note:*** You need to give your LAN PC clients a fixed/ static IP address for the Access Control rule to work properly.
Client PC Service	You can block clients from accessing some Internet services by checking those you want to block.
Protocol	Select "UDP," "TCP" or "Both."

Port Range	You can enter (then click “Add”) up to five port ranges. The router will block clients from accessing Internet services that use these ports.
Reset	Click “Reset” to clear all fields.

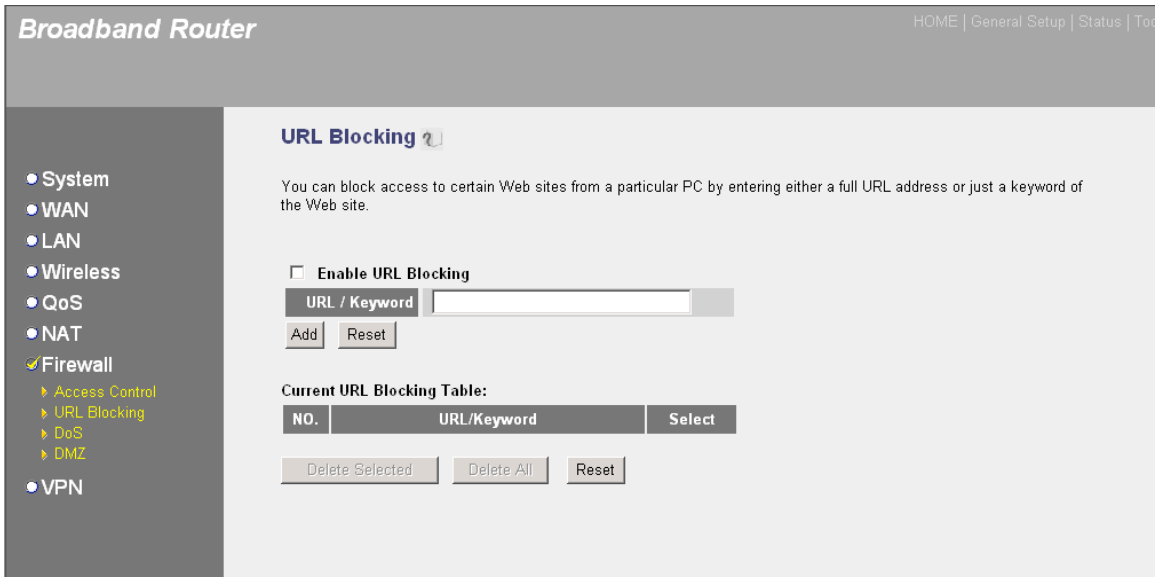
Click “Apply Changes” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

Example: Access Control
In the example below, LAN client A can only access websites that use Port 80. However, LAN client B is able to access websites and any other service that uses ports between 80 and 999.



3.7.2 URL Blocking

Access can block access to some Web sites from particular PCs by entering a full URL address or just keyword of the Web site.

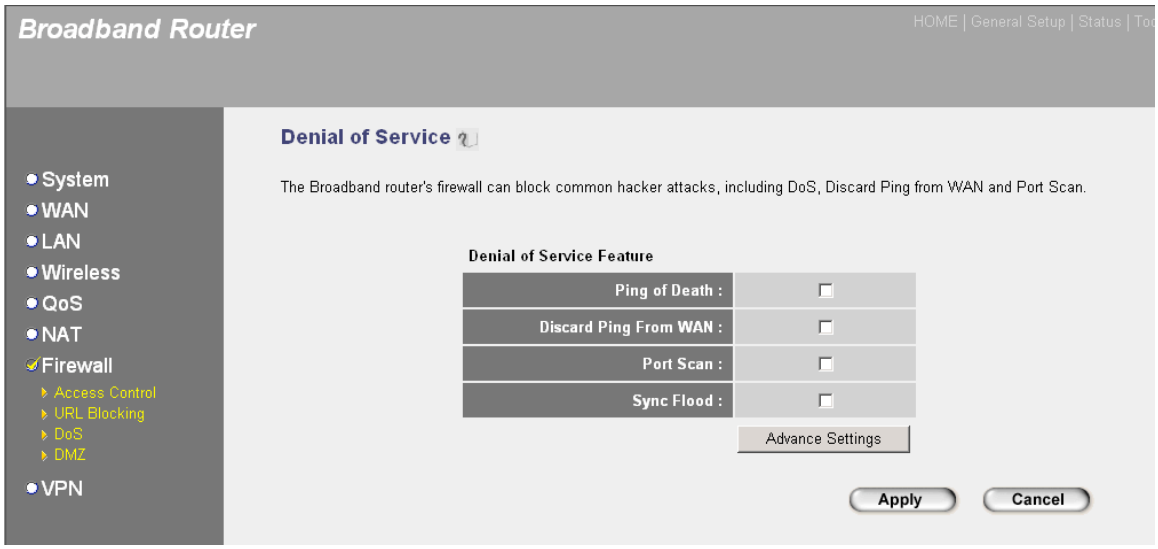


Parameter	Description
Enable URL Blocking	Select to activate the function.
Add URL Keyword	Fill in the “URL/Keyword” field and click “Add.” You can enter the full URL address or the keyword of the Web site you want to block. To change or correct an entry before adding it, click "Reset" and re-enter.
Remove URL Keyword	To remove a URL keyword from the Current URL Blocking Table, select it in the table and click "Delete Selected." To remove all URL keywords from the table, click "Delete All.” To clear the selection and re-select, click “Reset.”

You can now configure other advance sections or start using the router.

3.7.3 DoS

The router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur, the router can log the events.

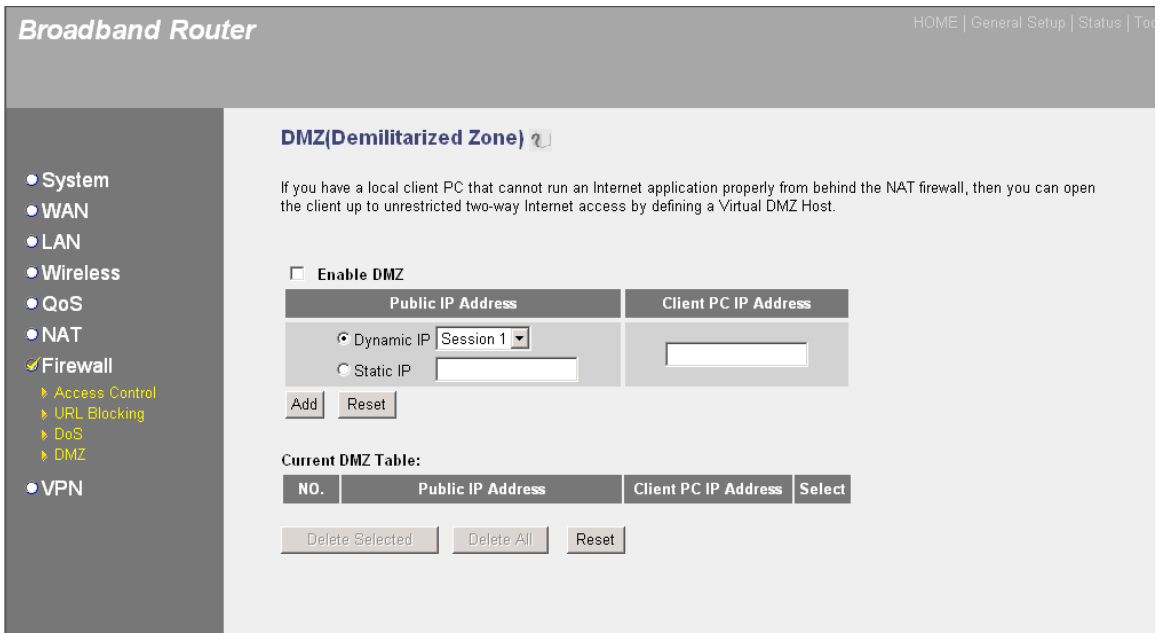


Intrusion Detection Feature	Description
Ping of Death	Protects from Ping of Death attack.
Discard Ping From WAN	The router's WAN port will not respond to any Ping requests.
Port Scan	Protects the router from Port Scan.
Sync Flood	Protects the router from Sync Flood attack.

Click "Apply" at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

3.7.4 DMZ

If you have a local client PC that cannot run an Internet application (e.g., games) properly from behind the NAT firewall, you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g., FTP, Web sites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

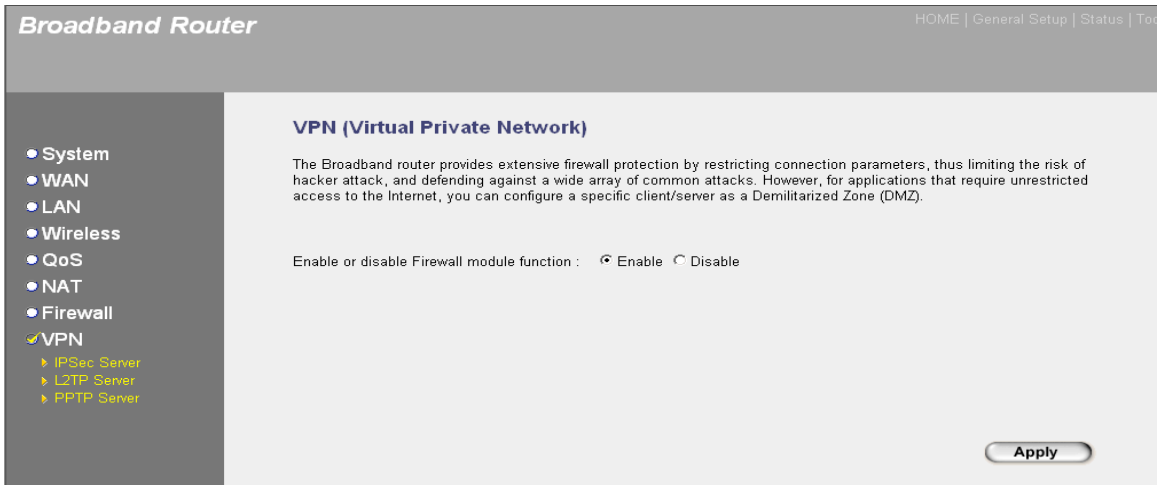


Parameter	Description
Enable DMZ	Select to enable the function. ***Note:*** If there is a conflict between the Virtual Server and the DMZ settings, the Virtual Server function will have priority over the DMZ function.
Public IP Address	Enter the IP address of the WAN port or any other public IP addresses given to you by your ISP.
Client PC IP Address	Enter the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port / public IP address above. ***Note:*** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

You can now configure other sections or start using the router.

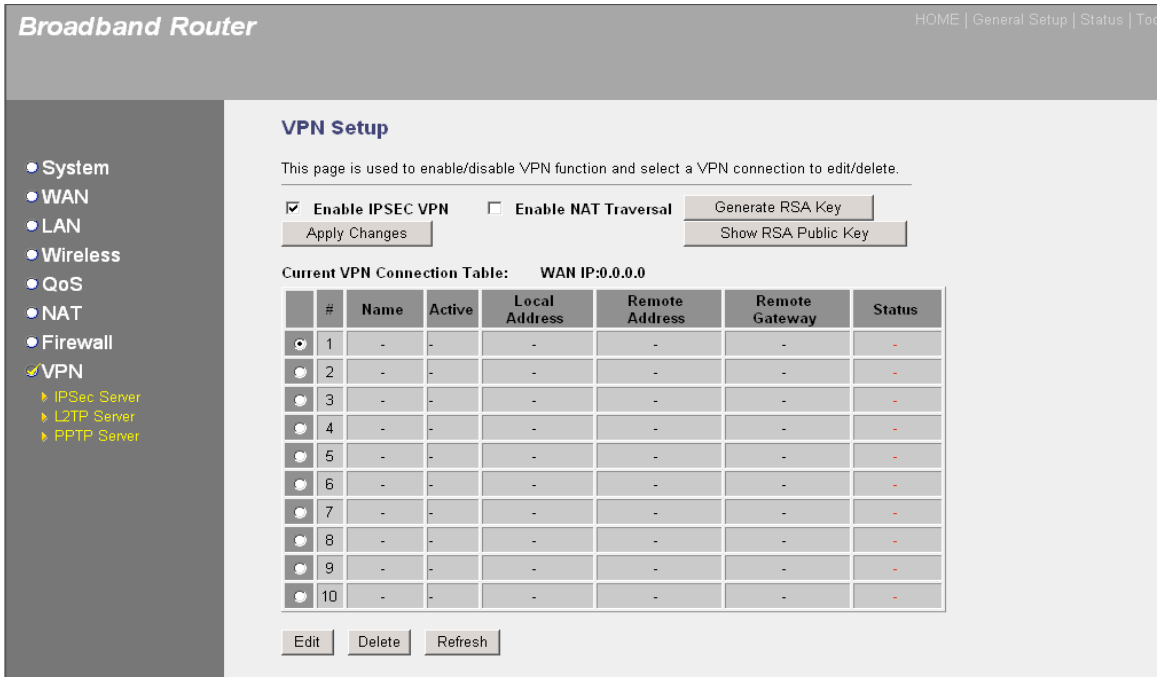
3.8 VPN

Virtual Private Network (VPN) provides a secure, private communication tunnel between two or more devices across the Internet. These VPN devices can be either a computer running VPN software or a special device like a VPN-enabled router. It allows your home computer to be connected to your office network or can allow two home computers in different locations to connect to each over the Internet. ***Note:*** To enable the VPN settings, select “Enable” and click “Apply.”

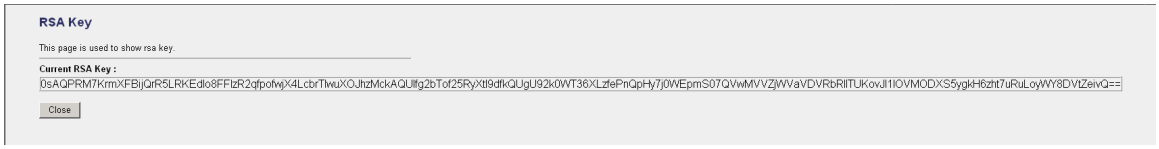


3.8.1 IPSec Server

IPSec (IP Security Protocol) is an extended IP protocol that enables secure data transfer. It provides services similar to SSL/TLS; however, these services are provided on a network layer.

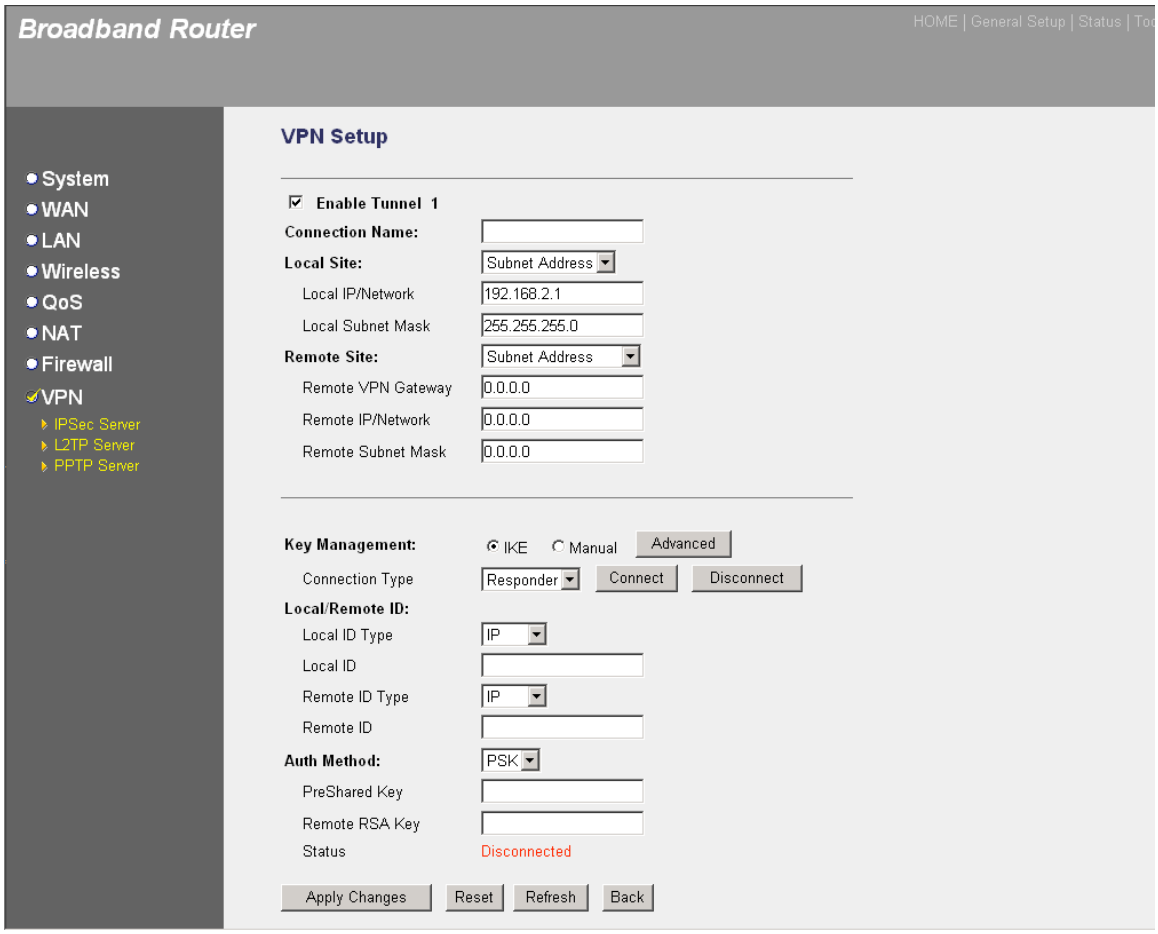


Parameter	Description
Enable IPSEC VPN	Select to activate the function.
Enable NAT Traversal	Enabling the NAT Traversal function allows clients behind NAT to connect to this VPN server.
Generate RSA Key	Click to automatically generate the RSA Public Key.
Show RSA Public Key	Click to show the RSA public key (below).



Current VPN Connection Table	This table shows the current tunnel settings and the status of each tunnel. The maximum number of tunnels is 10.
WAN IP	Shows the current WAN IP for this VPN server.
Edit a VPN Connection	Select the connection you want to edit and click “Edit.” You will enter the detail screen for the Tunnel Setting (below). Click “Apply Changes” after editing the form and the tunnel setting will be saved.

Edit Connection:

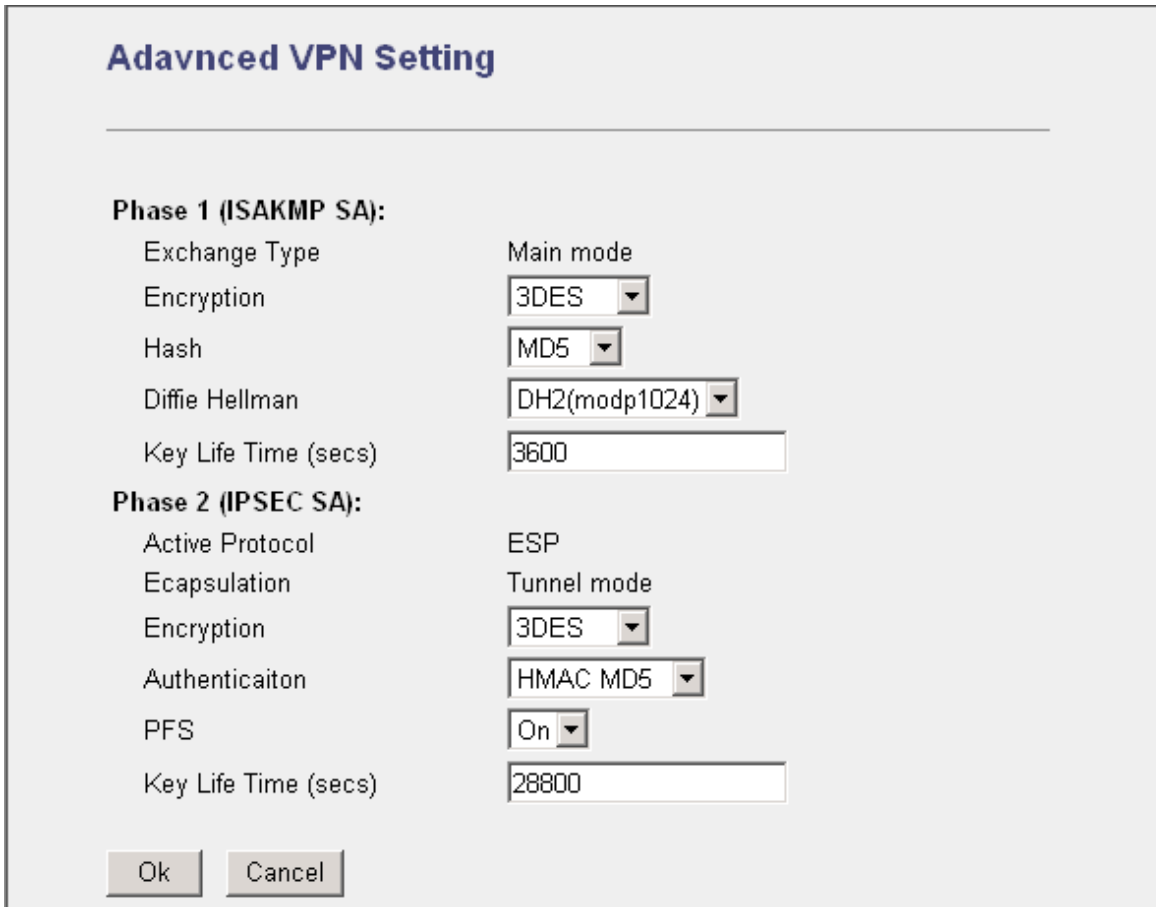


Parameter	Description
Enable Tunnel #	Select to enable this tunnel setting.
Connection Name	Enter a name for this connection. ***Note:*** Each of the names needs to be unique (not duplicated).
Local Site	Choose a type for the local site: single site or subnet.
Remote Site	Choose a type for the remote site: single site, subnet, any address, any NAT Traversal address or L2TP client. When you choose single site or subnet, you need to specify the remote IP address.
Network Management	Choose the key exchange method: “IKE” or “Manual.”
Advanced	Click for the advanced setting screen for IKE (below).
Connection Type	Select “Initiator” and the tunnel will automatically connect at the boot time. Select “Responder” and the

	tunnel will connect only when you click “Connect.”
Local/Remote ID	Specify the ID of the local and remote sites. It can be an IP address, domain name, or e-mail address.
Auth Method	Choose “PSK” or “RSA” and enter the key for the authentication.

Click “Apply Changes” at the bottom of the screen to save the above configurations. You can now configure other sections or start using the router.

Advanced VPN Setting:



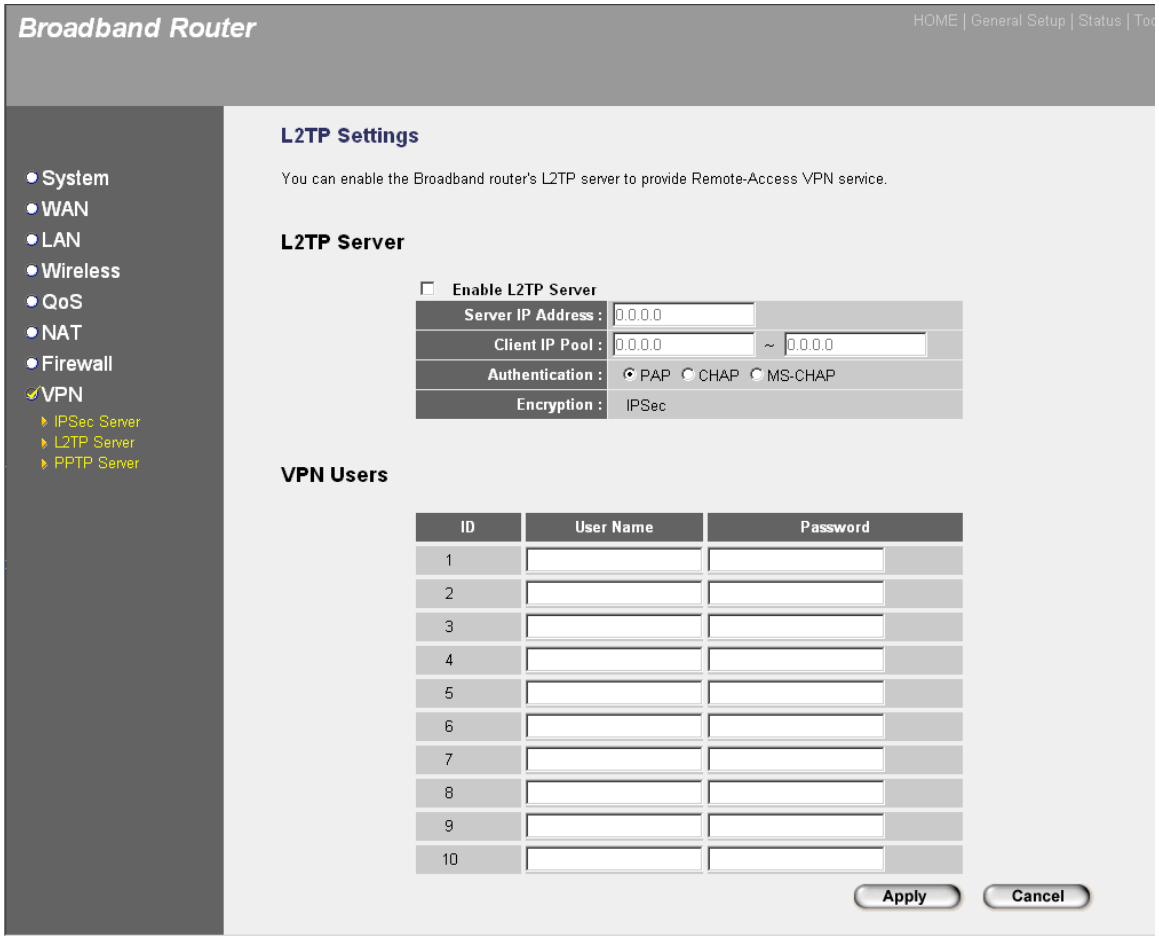
Parameter	Description
Encryption	Choose the encryption type with the remote peer: “3DES” or “AES128.” ***Note:*** If you choose the wrong method, the connection may not be established.
Hash/Authentication	Choose the hash method with the remote peer: “MD5” or “SHA1.” ***Note:*** If you choose the wrong method, the connection may not be established.

Diffie Hellman	Choose which Diffie Hellman protocol you want to use for Phase 1.
Key Life Time	Enter the life time for the key. After this time interval, the key will expire.
PFS	If you select “On,” the keys that protect data transmission are not used to derive additional keys. Also, seeds used to create data transmission keys are not re-used.

Click “OK” at the bottom of the screen to save the above configurations.

3.8.2 L2TP Server

The Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP). By enable this server, you can enable the operation of a virtual private network (VPN) over the Internet.

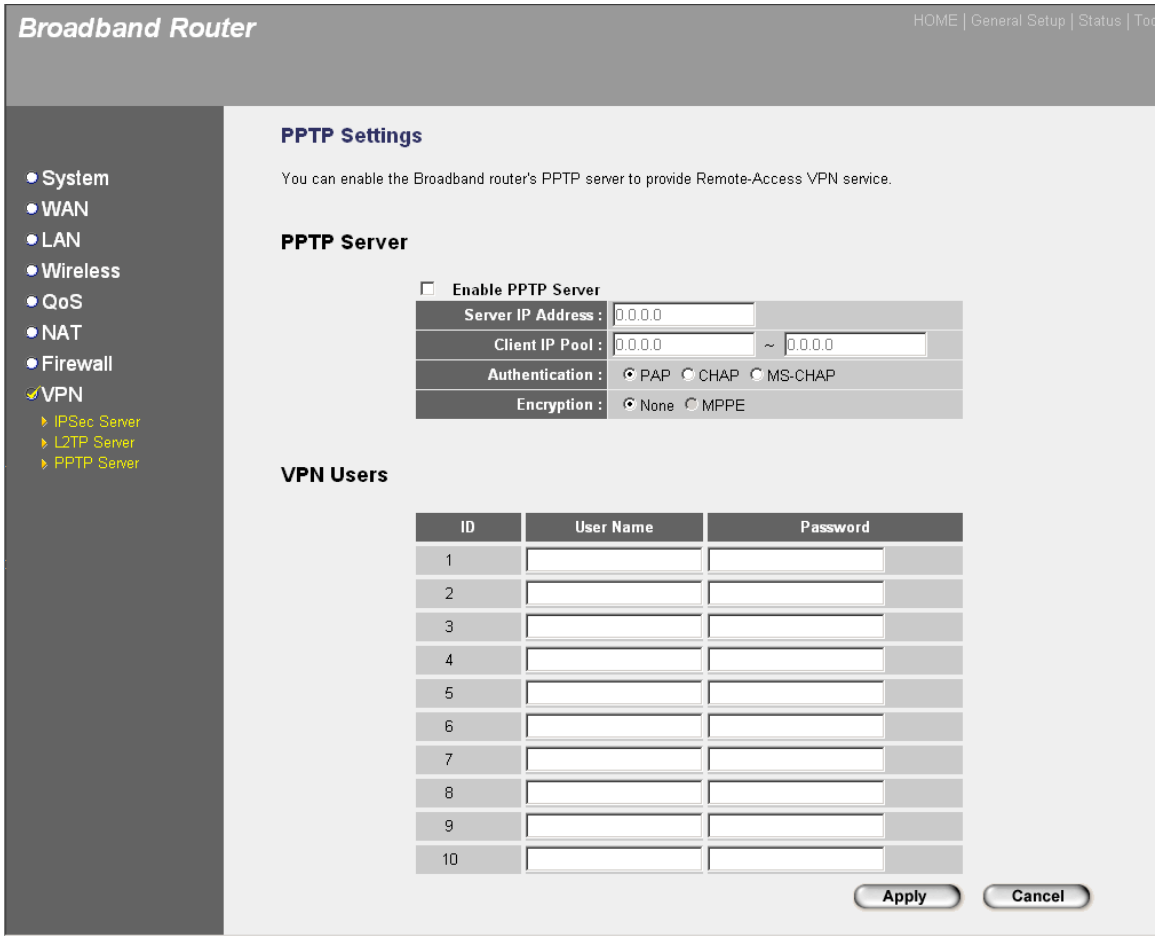


Parameter	Description
Enable L2TP Server	Click to enable the operation of a virtual private network (VPN) over the Internet.
Server IP Address	Specify the IP address the L2TP clients communicate with. ***Note:*** The Server IP Address can be different from the LAN IP or WAN IP.
Client IP Pool	Specify the IP address for L2TP clients to use.
Authentication	Select “PAP,” “CHAP” or “MSCHAP.”
VPN Users	Enter up to 10 usernames and passwords for the L2TP / PPTP clients.

Click “Apply” at the bottom of the screen to save the above configurations.

3.8.3 PPTP Server

PPTP is a protocol from Microsoft that is used to create a virtual private network (VPN) over the Internet. It uses Microsoft's Point-to-Point Encryption (MPPE), which is based on RSA's RC4.

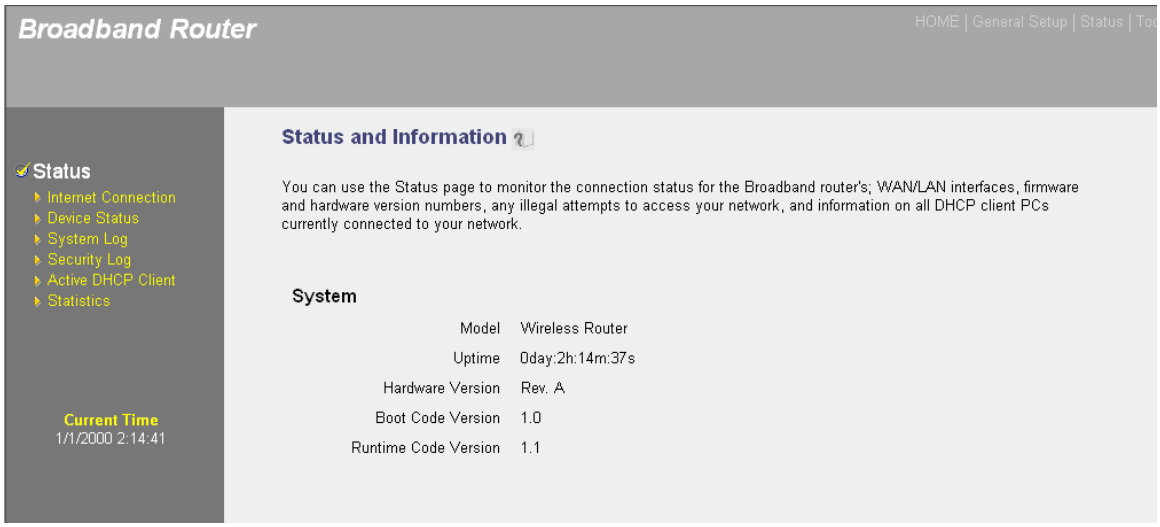


Parameter	Description
Enable PPTP Server	Click to enable the operation of a virtual private network (VPN) over the Internet.
Server IP Address	Specify the IP address PPTP clients communicate with. ***Note:*** The Server IP Address can be different from the LAN IP or WAN IP.
Client IP Pool	Specify the IP address for PPTP clients to use.
Authentication	Select “PAP,” “CHAP” or “MSCHAP.”
Encryption	When you choose “MSCHAP” for Authentication, you can use “MPPE” (Microsoft's Point-to-Point Encryption) to encrypt the PPTP connection.
VPN Users	Enter up to 10 usernames and passwords for the L2TP / PPTP clients.

Click “Apply” at the bottom of the screen to save the above configurations.

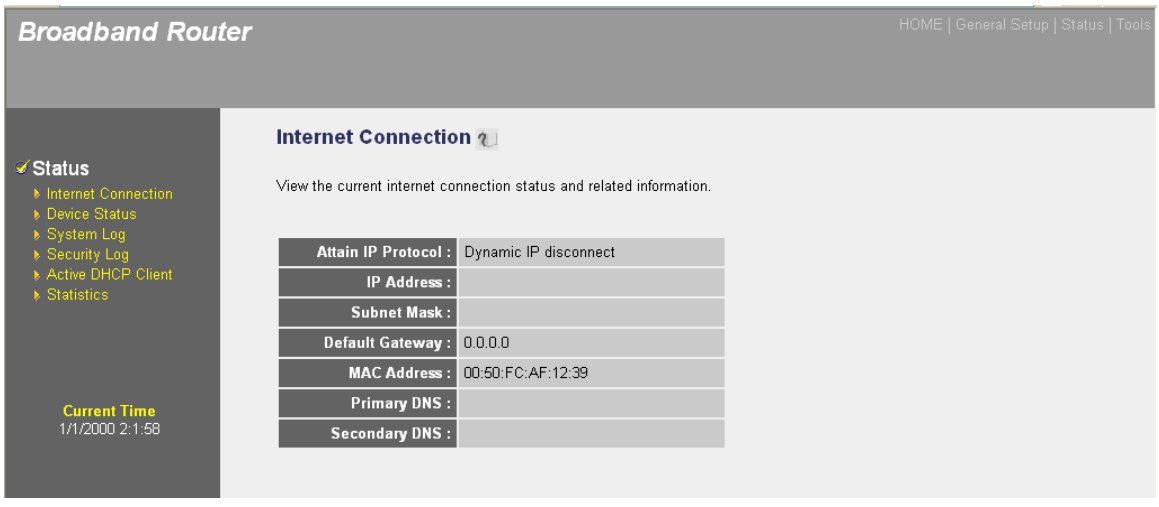
4 STATUS

The Status section allows you to monitor the current status of your router: WAN/ LAN interface connections, the current firmware and hardware version numbers, any illegal attempts to access your network, information on all DHCP client PCs currently connected to your network, and more.



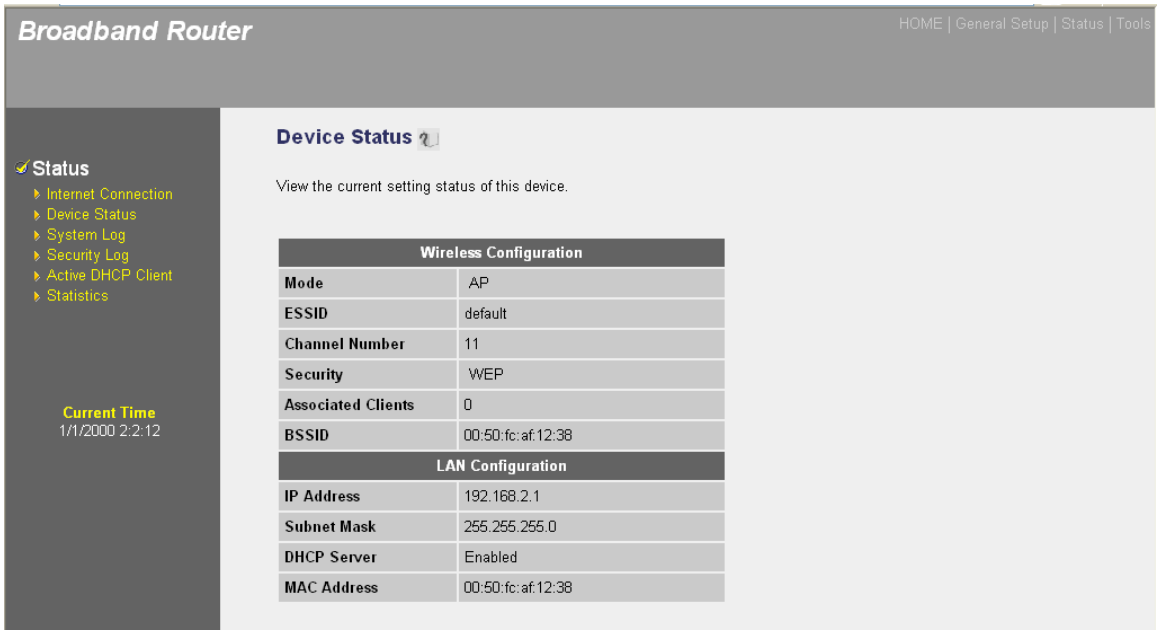
4.1 Internet Connection

View the router's current Internet connection status and other related information, such as whether the WAN port is connected to a cable/DSL connection; the WAN IP address, subnet mask and ISP gateway; and the primary and secondary DNS being used.



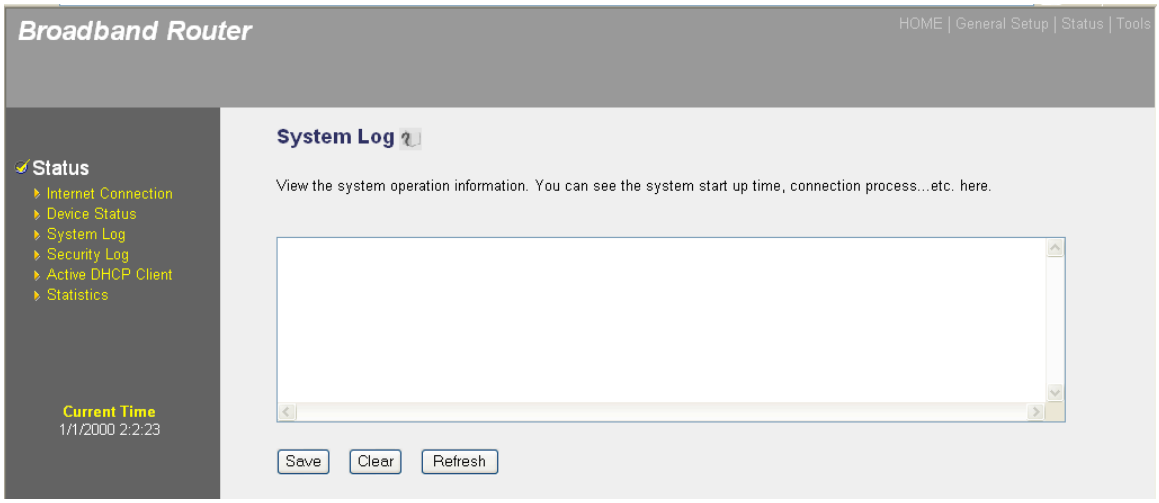
4.2 Device Status

View the router's current configuration settings established in the Quick Setup Wizard and/or General Setup sections, such as the LAN port's current LAN IP address and subnet mask, and whether the DHCP Server function is enabled or disabled.



4.3 System Log

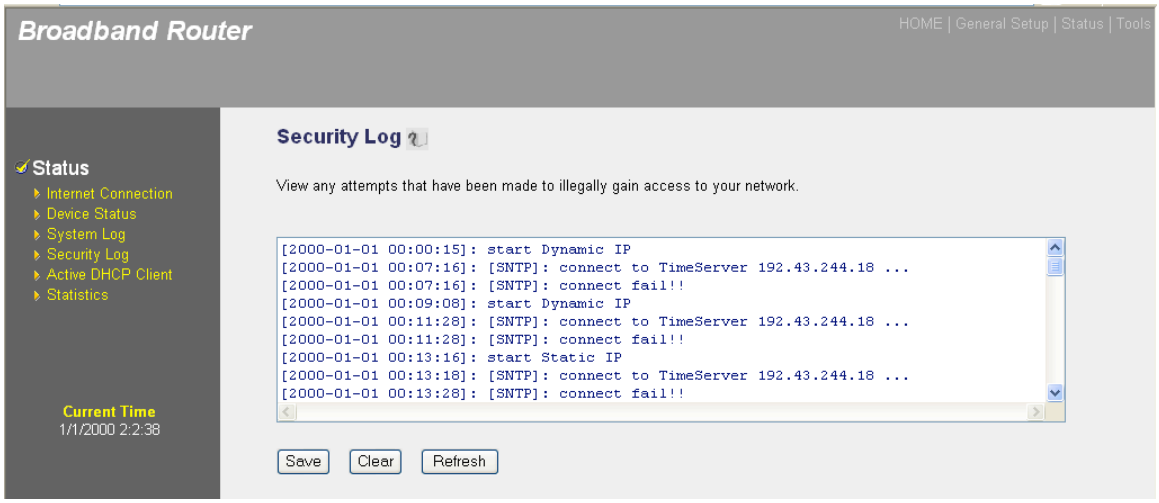
View the operation log of the system, including any event that has occurred since system startup. When the system is powered down, the system log will disappear if not saved to a local file.



Parameter	Description
Save	Click to save the system log to a local file for further processing.
Clear	Click to clear the log entries.
Refresh	Click to get the most updated situation.

4.4 Security Log

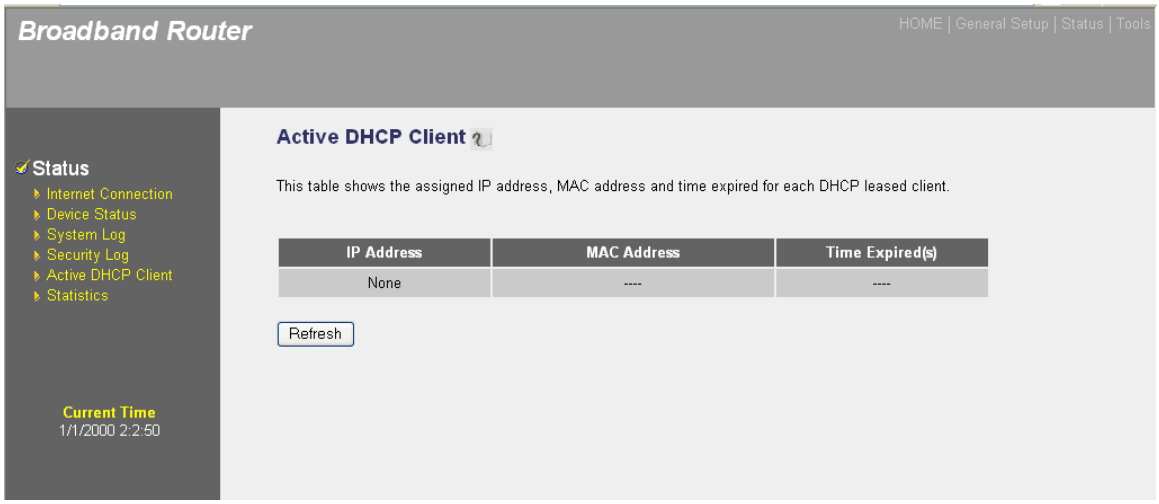
View any attempts that have been made to illegally gain access to your network. When the system is powered down, the security log will disappear if not saved to a local file.



Parameter	Description
Save	Click to save the security log to a local file for further processing.
Clear	Click to clear the log entries.
Refresh	Click to get the most updated situation.

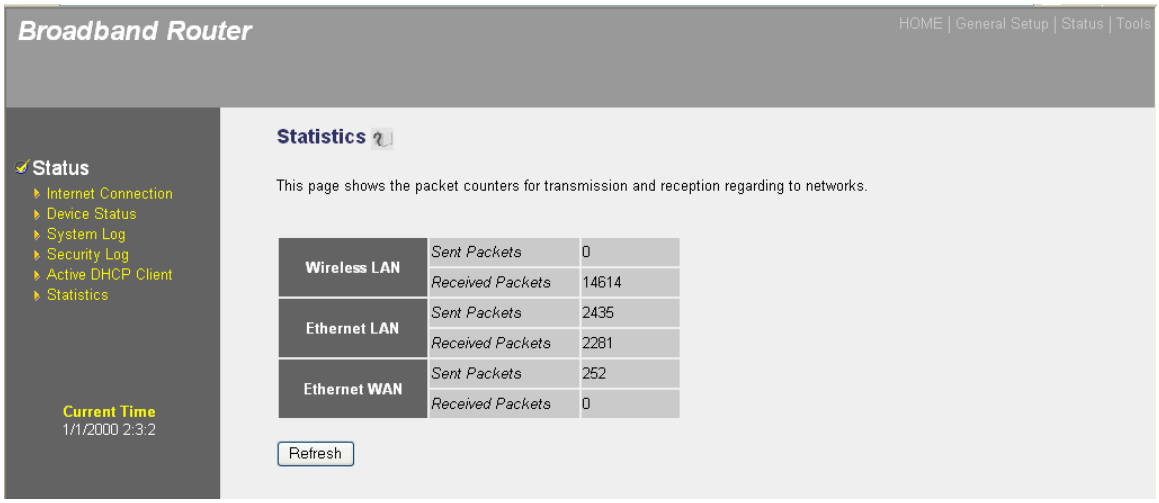
4.5 Active DHCP Client

View your LAN client's information that is currently linked to the router's DHCP server. The Active DHCP Client Table displays the IP address, the MAC address and Time Expired of each LAN client. Click “Refresh” to get the most updated situation.



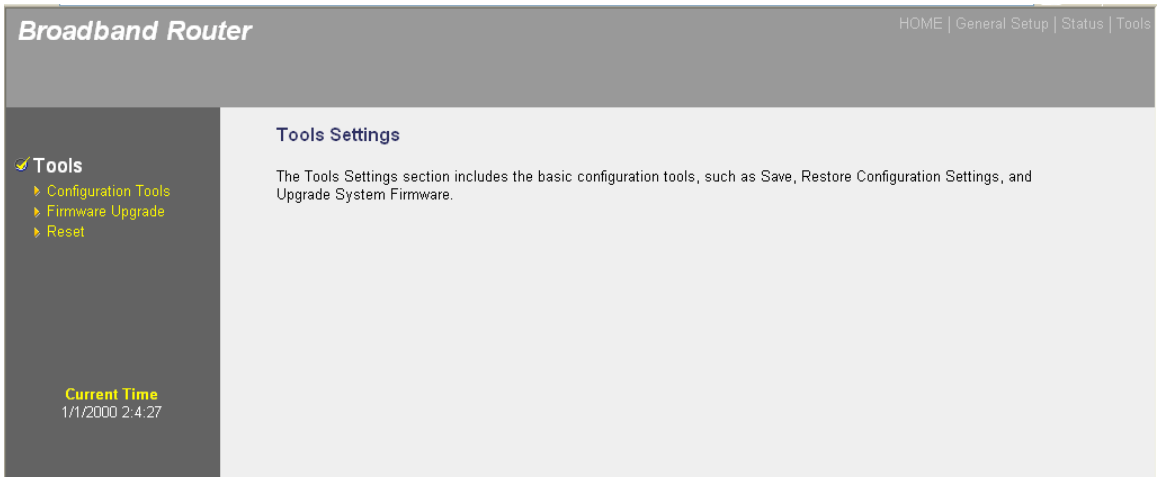
4.6 Statistics

View the statistics of packets sent and received on WAN, LAN and wireless LAN. Click “Refresh” to get the most updated situation.



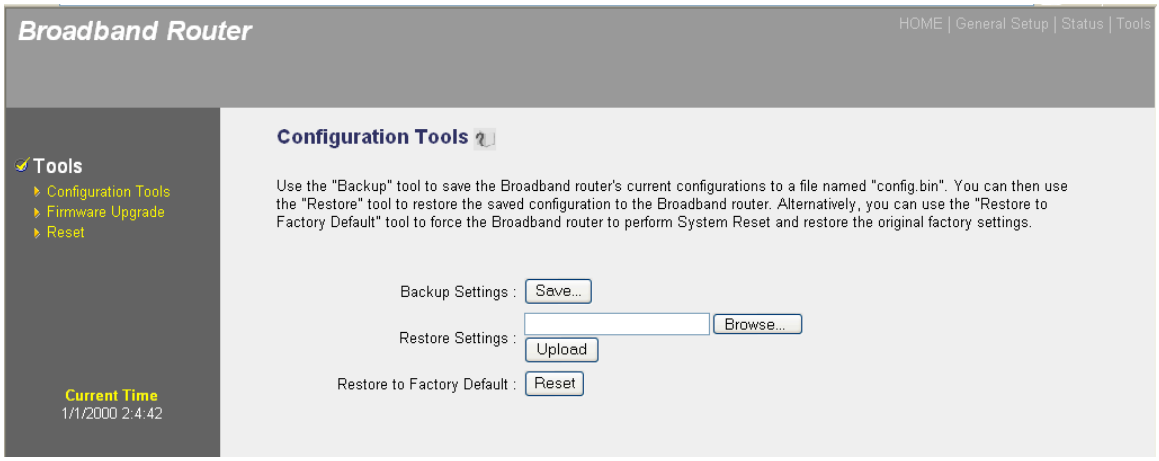
5 TOOLS

This section presents three basic, but important, sub-sections: Configuration Tools (to save or restore configuration settings), Firmware Upgrade (to upgrade system firmware) and Reset.



5.1 Configuration Tools

This screen allows you to save (back up) the router's current configuration, which provides added protection and convenience should problems occur and you need to reset to factory defaults. When the configuration has been saved, you can re-load the settings into the router.



Parameter	Description
Back Up Settings	Click "Save" to save the router's current configuration to a file named "config.bin" on your PC.

Restore Settings	Click “Upload” to restore the saved configuration to the router.
Restore to Factory Defaults	Click “Reset” to force the router to perform a power reset and restore the original factory settings.

5.2 Firmware Upgrade

This screen allows you to upgrade the router’s firmware. Download the firmware file to your local hard disk, then enter that file name and path in the appropriate field on this screen. You can also click “Browse” to find the firmware file on your PC. Once you’ve selected the new firmware file, click “Apply” at the bottom of the screen to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete.) Once the upgrade is complete, you can start using the router.

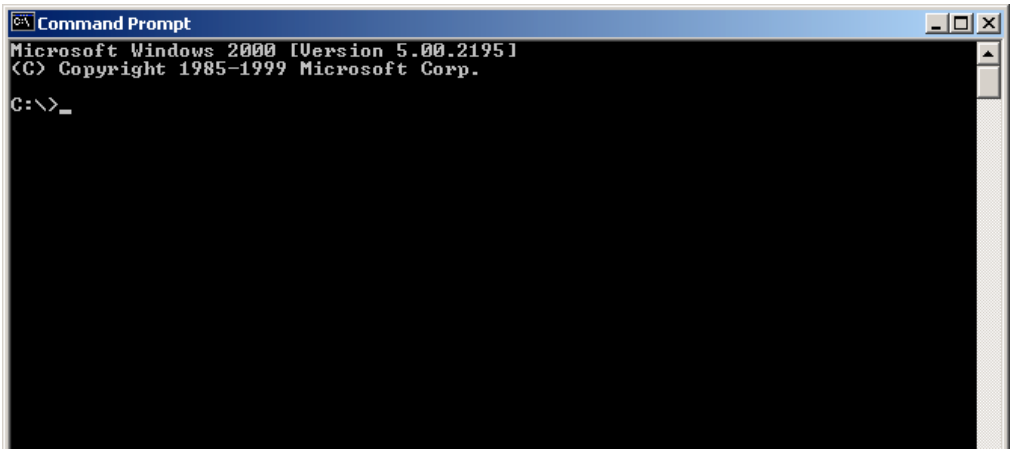
5.3 Reset

The reset function essentially re-boots your router’s system, which may be necessary in the event the system stops responding correctly or in some way stops functioning. Your settings will not be changed. To perform the reset, first click “Apply.” You’ll be asked to confirm your decision. The reset will be complete when the power light stops blinking. Once the reset process is complete, you can start using the router again.

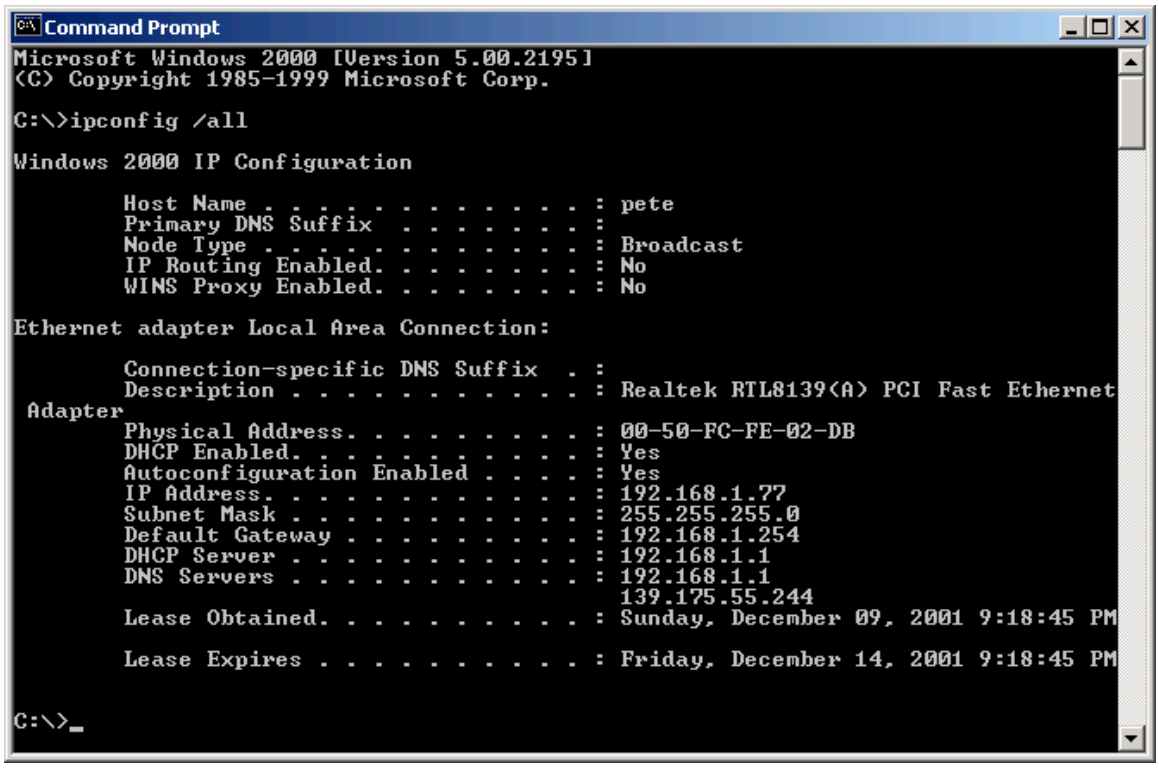
APPENDIX

This shows you how to manually find your PCs IP and MAC addresses.

1. In Windows, open the Command Prompt program



2. Type “Ipconfig /all” and press <Enter>.



- Your PC’s IP address: 192.168.1.77
- The router’s IP address: Default Gateway 192.168.1.254
- Your PC’s MAC address: Physical Address 00-50-FC-FE-02-DB

GLOSSARY

Default Gateway (Router): Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out toward the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.intellinet-network.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses so that when a domain name is requested (as in typing "intellinet-network.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods that identifies a single, unique Internet computer host in an IP network.

Example:

192.168.2.1 consists of two parts: an IP network address and a host identifier. The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255; or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.

A network (subnet) mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore, sometimes a network mask can also be described simply as "x" number of leading 1's. When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

Example:

If the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is

11111111.11111111.11110000.00000000, it means the device's network address is 11011001.10110000.10010000.00000000, and its host ID is 00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: (see ISP). This is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network, serving as a unique identifier for a device with an Ethernet interface. It is composed of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes often used as the product's serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using this router's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. This is a secure data-transmission method originally created for dial-up connections; PPPoE is for Ethernet connections, and relies on two widely accepted standards: Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

Protocol: A protocol is a set of rules for interaction agreed upon among multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information, such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g., 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocols. TCP performs proper error detection and error recovery, and thus is reliable. UDP, on the other hand, is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network is a network that connects computers located in geographically separate areas (e.g., different buildings, cities, countries). The Internet is a wide area network.

Web-Based Management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the Web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

SPECIFICATIONS

Standards
• IEEE 802.1d (Spanning Tree Protocol)
• IEEE 802.1x (Wireless User Authentication)
• IEEE 802.11b (11 Mbps Wireless LAN)
• IEEE 802.11g (54 Mbps Wireless LAN)
• IEEE 802.3 (10Base-T Ethernet)
• IEEE 802.3u (100Base-TX Fast Ethernet)

General
• LAN ports: 4 RJ45 10/100 Mbps data ports
• LAN ports with Auto MDI/MDI-X
• Flash: 4 MB
• Memory: 16 MB SDRAM
• Certifications: FCC Class B, CE Mark, RoHS

Router
• Chipset: Realtek RTL8186
• Supported WAN connection types:
  - Dynamic IP (DHCP for cable service)
  - Static IP
  - PPPoE (for DSL)
  - PPTP
  - L2TP
  - Telstra BigPond
• Protocols:
  - CSMA/CA
  - CSMA/CD
  - TCP/IP
  - UDP
  - ICMP
  - PPPoE
  - NTP
  - NAT (network address translation)
  - DHCP
  - DNS
• NAT:
  - Port forwarding
  - Virtual server
  - Special applications (port trigger)
• Firewall:
  - URL blocking
  - Anti-DoS protection against ping of death, port scans, syn flood)

- Access control based on MAC address
- DMZ (demilitarized zone)

• Supports UPnP (Universal Plug and Play)
• Supports DHCP (client/server)

Wireless

• Chipset: RTL8225
• Wireless frequency range: 2.412 - 2.484 GHz
• Modulation technologies:
- 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
- 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM

• Number of channels: 13
• Data rates:
- IEEE 802.11b (11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps)
- IEEE 802.11g (54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, 6 Mbps)

• Output power:
- OFDM: 15 dBm +/- 1 dBm (54 Mbps, 50 mW max.)
- CCK: 17 dBm +/- 1 dBm (11 Mbps, 50 mW max.)

• Maximum coverage distance: 100 m / 300 ft. (indoor), 300 m / 900 ft. (outdoor)
• Wireless security:
- WEP encryption (64/128-bit)
- WPA TKIP
- WPA2 AES
- WPA2 mixed
- WPA RADIUS
- Client access control through media access control (MAC) filter

• Antenna: single detachable dipole antenna with RP-SMA connector, 2 dBi gain

VPN

• Supports VPN PPTP and IPsec pass-through
• 10 VPN user accounts
• VPN server protocol support: PPTP, IPSec and L2TP
• 3DES and AES encryption
• MD5 and SHA1 authentication

QoS

• Definition of total upload and download bandwidth
• Custom rules for maximum bandwidth or minimum guaranteed bandwidth
• Individual rules for upload and download
• Rules can be applied for IP addresses, ports, port ranges, UDP/TCP and traffic types (SMTP, HTTP, POP3, FTP)

LEDs

• Power

• WLAN Link/Act
• WAN Link/Act
• WAN 10/100 Mbps
• LAN 1-4 Link/Act
• LAN 1-4 10/100 Mbps

Environmental
• Dimensions: 187 (W) x 100 (L) x 30 (H) mm (7.4 x 3.9 x 1.2 in.)
• Weight: 0.8 kg (1.7 lbs.)
• Operating temperature: 0 – 40°C (32 – 104°F)
• Operating humidity: 10 – 90% RH, non-condensing
• Storage temperature: -20 – 60°C (4 – 149°F)

Power
• External power adapter: 12 V DC, 1.0 A
• Power consumption: 5.5 Watts max.

Package Contents
• Wireless G 4-Port VPN Router
• User manual
• Power adapter
• Ethernet Cat5 RJ45 cable, 1.0 m (3 ft.)